APLICACIÓN DE METODOLOGÍAS DE GENERACIÓN DE POLITICA Y DE GESTIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN COMO CASO DE ESTUDIO EN UNA EMPRESA DE TELEINFORMATICA EN LA CIUDAD DE BOGOTA D.C.

GUILLERMO RODRÍGUEZ GAHONA

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA DE SISTEMAS Y DE LA COMPUTACIÓN

PEREIRA/RISARALDA

JULIO DE 2014

APLICACIÓN DE METODOLOGÍAS DE GENERACIÓN DE POLITICA Y DE GESTIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN COMO CASO DE ESTUDIO EN UNA EMPRESA DE TELEINFORMATICA EN LA CIUDAD DE BOGOTA D.C.

GUILLERMO RODRÍGUEZ GAHONA

COAUTORA: INGENIERA PAULA ANDREA VILLA SÁNCHEZ

Trabajo de grado para optar al título de Ingeniero de sistemas y Computación

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

FACULTAD DE INGENIERÍAS

PROGRAMA DE INGENIERÍA DE SISTEMAS Y DE LA COMPUTACIÓN

PEREIRA/RISARALDA

JULIO DE 2014

Nota de aceptación

_____

_____

_____

_____

Presidente del jurado

_____

Jurado

_____

Jurado

Pereira/Risaralda, julio de 2014

DEDICATORIA

A la mujer de mi vida, mi esposa, por sus palabras, su confianza, por su amor, su aporte moral, espiritual y profesional en la culminación de este proceso.

AGRADECIMIENTOS

El presente trabajo de grado está dedicado a mi madre por sus oraciones en silencio, a mis hermanos y hermanas por su confianza.

A mi familia por sus buenos deseos, a mi prima por impulsarme y alentarme para empezar este camino, a mis amigos, compañeros y todas aquellas personas que contribuyeron al logro de este objetivo.

Agradezco a la empresa por permitirme realizar el presente trabajo investigativo.

A cada uno de los miembros de la organización por su aporte en el desarrollo de los diversos instrumentos y herramientas, que debieron diligenciar y trabajar, para consolidar la política de seguridad de la información.

A los dueños de los procesos de la empresa, por el aporte significativo en el desarrollo del inventario de los activos de la información y en el mapa de riesgos.

A los miembros del comité de seguridad, por la contribución relevante en el adelanto y consolidación de los objetivos del proyecto.

Y finalmente, a la Ingeniera Paula Andrea Villa, por la tutoría y acompañamiento en el proceso.

TABLA DE CONTENIDO

TABLA DE GRAFICOS

INDICE DE TABLAS

INTRODUCCIÓN

Los sistemas seguridad de la información son hoy en día de importancia y relevancia para la mayoría de las organizaciones; toda vez que impiden fugas o posibles incidentes de información que pueden ocasionar daños irreparables para los objetivos organizacionales, tal es el caso de robos de información que han generado que algunas empresas pierdan clientes, que el valor agregado de los productos que ofrecen sea conocido por otras organizaciones, e incluso que la competencia conozca la información privada o estrategias de marketing con anterioridad.

Todo ello, lleva a que las instituciones internacionales como el caso de la ISO genere una normatividad, acompañada de lineamientos y procedimientos que faciliten la implementación de los llamado SGSI, que han denominado la serie 27000 y más recientemente la 31000, que permiten en su concurso llevar a término un sistema de gestión en lo relativo a la seguridad de la información

La ingeniería de sistemas como profesión responsable de gestar y diseñar procesos relacionados con la arquitectura e infraestructura informacional de una empresa, debe dar cuenta de la protección y resguardo de la información en las organizaciones; esta y otras más son las razones por las cuales los ingenieros de sistemas son los llamados a liderar los SGSI; en este sentido la Universidad Tecnológica de Pereira asume el reto de formar, investigar e innovar en lo relativo a este tema y con la vanguardia del grupo de investigación Nyquist se crea la metodología para la generación de una política de seguridad de la información.

Dicha metodología se constituye en el insumo fundamental para el desarrollo del presente proyecto de investigación, pretende validar la metodología diseñada por el grupo de investigación Nyquist, en el caso específico de la empresa:, ubicada en la ciudad de Bogotá, dedicada servicio de productos de

telecomunicaciones y que en actualidad se muestra como una pequeña empresa, pero en proceso de expansión, debido a los nuevos clientes, que son cada vez más importantes en el sector público y privado y que le exigen algunos requerimientos en la confidencialidad y el manejo de la información.

En este sentido, la empresa, se constituye en un espacio abierto para implementar la metodología y en general diseñar un Sistema Gestión de Seguridad de la Información, que satisfaga las necesidades particulares de la empresa y sus clientes, permitiendo de este modo validar la metodología del grupo de investigación señalado anteriormente.

Este documento final, da cuenta de la ejecución e implementación del proyecto de investigación, el lector encontrará en el primer capítulo los preliminares de la investigación, en el que se establece la justificación del proyecto, objetivos, hipótesis y metodología del mismo, destacándose las fases y procedimientos que se llevarán a cabo en el ejercicio investigativo, en especial se delimita que uno de los productos finales y el más importante es la generación de la política de seguridad de la información.

En el segundo capítulo, se realiza un análisis diagnóstico de la empresa. Sobre la seguridad de la información, a través de una encuesta que se aplica a todos y cada uno de los miembros de la organización; resultado que se presenta en forma cuantitativa y cualitativa y evidencia la situación de la empresa en lo relativo al manejo y protección de la información. Para la elaboración de la encuesta el insumo lo constituyen las normas 27000 y 27001.

En el tercer y cuarto capítulo se encontrará la implementación de la metodología para la generación de la política de seguridad de la información diseñada por el grupo Nyquist, con la elaboración del proyecto que se presenta a la empresa y la ejecución paso a paso del mismo, que va desde asignar al oficial de seguridad de la información hasta generar la política.

La política generada se encuentra establecida en el capítulo cuarto y atiende a las particularidades de la empresa y es validada aprobada, socializada y multiplicada al interior de toda la organización.

En el quinto capítulo se halla lo correspondiente a la implementación de la metodología de gestión del riesgo, interdependiente y complementaria de la política de seguridad, en este apartado se encuentra la matriz y mapa de riesgos, que permite evidenciar las posibles amenazas a los activos de la información, los controles necesarios para impedir los incidentes y los procedimientos en caso de que se generen dichos incidentes; es importante aclarar que este capítulo responde a complementar y consolidar la política de seguridad de la información de la empresa.

En el sexto capítulo se evidencian los resultados de aplicar nuevamente la encuesta de diagnóstico, después de generar la política, capacitar y sensibilizar a todos los miembros de la organización sobre la importancia de gestar una cultura de seguridad de la información. Los cambios son drásticos y demuestran resultados significativos positivos.

Finalmente, las conclusiones dan cuenta de la validación de la hipótesis y el logro de los objetivos; al igual que los anexos permiten evidenciar la aceptación del proceso por parte de la organización y sus miembros en general.

1. TITULO

APLICACIÓN DE METODOLOGÍAS DE GENERACIÓN DE POLITICA Y DE GESTIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN COMO CASO DE ESTUDIO EN UNA EMPRESA DE TELECOMUNICACIONES EN LA CIUDAD DE BOGOTA D.C.

2. DEFINICIÓN DEL PROBLEMA

2.1. ANTECEDENTES DEL PROBLEMA

La Seguridad Información es una realidad sobre la cual los expertos y conocedores en el área han puesto su atención en el último tiempo, debido a la presencia cada vez mayor, constante y múltiple de vulnerabilidades técnicas, procedimentales y humanas, que han llamado la atención en las grandes, medianas y pequeñas empresas, para lo cual ha sido importante y en algunos casos, casi que obligatorio establecer de alguna manera directrices y políticas de seguridad formales, para tratar de reducir los riesgos que afecten la información en las organizaciones.

La misión de la empresa consiste principalmente en el desarrollo de soluciones tecnológicas en el sector de la Teleinformática, prestando sus servicios a entidades del sector público y privado, tales como corporaciones bancarias, call center, empresas del sector público, centrales de taxis, entre otras, por ello, el cumplimiento de las exigencias en cuanto a la seguridad de la información es esencial para la prestación de los servicios a dichos clientes, especialmente cuando se trata de entidades bancarias en las que el cumplimiento de normas y leyes debe ser por conexión[1].

No obstante La empresa, hasta la fecha no ha presentado incumplimiento a los requerimientos establecidos por los clientes externos en relación a la seguridad de

[1]La entidades bancarias y financieras, al igual que las empresas del Estado, deben tener en cuenta entre otras las siguientes leyes, que la empresa de estudio por ser uno de sus proveedores, también debe considerar: derechos de autor (decisión 351 de3 la C.A.N., ley 23 de 1982, decreto 1360 de 1989, la ley 44 de 1993, decreto 460 de 1995, decreto 162 de 1996, ley 545 de 1999, ley 565 de 2000, ley 603 de 2000, ley 719 de 20001), propiedad industrial (decisión 486 de la C.A.N., decreto 2591 de 2000, ley 463 de 1998, ley 170 de 1994, ley 178 de 1994) propiedad intelectual (decisión 345 de la C.A.N, decisión 391 de la C.A.N, decisión 523 de la C.A.N.) comercio electrónico y firmas digitales (ley 527 de 1999, decreto 1747 de 2000, resolución 26930 de 2000), La ley 1273 de 2009, que agrega dos capítulos referentes a la seguridad de la información en el código penal colombiano, en los que se señala los atentados contra la confidencialidad, la integralidad de los datos y sistemas colombianos y capítulo dos de los atentados informáticos y otras infracciones.

la información, pues se han establecido procedimientos que aunque no son normatizados[2], bajo un SGSI han logrado satisfacer los requerimientos específicos del cliente.

Por otro lado, en los más de catorce años que lleva en funcionamiento La empresa., en especial en los últimos años, se han presentado algunos incidentes significativos en lo que respecta a la seguridad de la información, tales como: el ataque constante de virus (lo cual se evidencia en el log del antivirus empresarial), el plagio de código fuente por personal de la empresa entre otros.

Especificando la situación de los incidentes y la vulnerabilidad de la seguridad de la información, en la empresa de servicios en teleinformática se destacan principalmente; los problemas eléctricos no documentados en los que por saltos de la regulación eléctrica algunos equipos se apagan borrando información, esto sucede de manera esporádica a pesar de los controles y revisiones realizadas al flujo eléctrico. En otro aspecto relacionado con la seguridad de la información no existen procedimientos y registros formales que permitan el manejo centralizado del código fuente, lo que hace que este quede al manejo libre de los miembros de la organización; igualmente no se lleva un adecuado control de cambios en lo que respecta al código fuente y a los proyectos que de la misma manera es de libertad para cada miembro de la empresa, situación que conlleva a dificultades en la trazabilidad de los proyectos y de la información de cada cliente externo.

Por otro lado, se puede caracterizar los tipos de fallos de la seguridad de la información en la empresa, así, 50 incidentes relacionados con virus, 50 más en lo referentes a ataques en la web y 50 en accesos a software dañinos, el incidente más importante ocurre con el robo a la información por parte de un miembro de la organización hurtando el código fuente de unos de los software pioneros y con el

[2] El manejo de seguridad de la información en la empresa. para clientes externos se toma según los requerimientos puntuales de estos; pero no existen procesos, procedimientos, registros documentados que sustenten un sistema de seguridad de la información, que hasta la fecha se ha podido sobrellevar de esta forma, pero debido al crecimiento de empresa y en especial al tipo de clientes –grandes entidades financieras y del Estado- se hace necesario un sistema que responda a nuevos requerimientos legales y normativos y ofrezca un valor agregado en las licitaciones y demás.

cual crea una nueva compañía, que se convierte en la actualidad competencia de la empresa.

De esta manera, la empresa, considera necesario emprender el ambiente para la construcción de un sistema de gestión de seguridad de la información, que le permita satisfacer las necesidades de sus clientes, volverse más competitivo en el mercado y en especial brindar un ambiente propicio que permita garantizar en un mayor grado la seguridad de la información al tratarse de un activo vital para la empresa.

2.2. FORMULACIÓN DEL PROBLEMA

Por lo indicado anteriormente, el presente proyecto pretende desarrollarse a partir de la siguiente pregunta:

La empresa necesita mejorar la seguridad de la información, ¿esto se puede lograr a través de la aplicación de metodologías de generación de política y de gestión de riesgos en seguridad de la información?

2.3. DESCRIPCIÓN DEL PROBLEMA

En lo referente, a las metodologías, controles y plan de implementación, la Universidad Tecnológica de Pereira, con el grupo de investigación Nyquist ha establecido como producto final de un proyecto de investigación en curso, el diseño de una metodología para la generación de política y la metodología de gestión de riesgos será seleccionada en el presente proyecto según la comparación de las mismas y las características de la empresa; estos serán el insumo para el desarrollo de la investigación que se llevará a cabo en la empresa, para resolver la pregunta anteriormente señalada.

De este modo, la investigación se constituirá en el inicio de un proceso, para la consolidación futura del SGSI en la empresa.

3. JUSTIFICACIÓN

El uso de la información en una empresa es fundamental para el logro de los objetivos; por ello los sistemas internacionales-ISO 27000, COBIT, ITIL Security[3]- han optado por establecer criterios, procesos y procedimientos que permitan en las organizaciones instituir un sistema información[4] tendiente a mantener confidencialidad y reserva de lo que se maneja dentro de las empresas u organizaciones.

Ya que día a día crece el cibercrimen y el ataque sobre la información[5] que administran cotidianamente las empresas, dichos ataques se realizan desde afuera, pero igualmente desde adentro, por ello la protección a la información debe ser rigurosa y compleja logrando asegurarla y estableciendo procesos y procedimientos claros y precisos, que impidan el robo, hurto o manejo inadecuado. En estudios recientes del año 2012, se ha concluido que en América Latina, Colombia obtuvo el tercer lugar en infecciones desde internet con un 7%, la preceden México con el 33% y Brasil con un 41%; en lo que respecta a las infecciones locales fuera de línea (a través de dispositivos USB y otros medios de

[3] La serie ISO 27000 son normas internacionales para la implantación de Sistemas de Gestión de Seguridad de la Información, el COBIT se refiere a las mejores prácticas en lo relacionado con la gestión de seguridad de la información y el ITIL Security es una marco de las mejores prácticas en información y su seguridad, practicadas en los años 80`s principalmente en los países europeos.

[4] Se entiende por sistema de información lo señalado por Vicente Aceituno Canal, en su libro *Seguridad de la información* lo siguiente: "…… información, mensajes, servicios, e interfaces como los activos representativos que componen los sistemas de información. Las funciones elementales que realizan los sistemas de información son el proceso, el almacenamiento, la comunicación y la entrada/salida de información" pág. 7

[5] En el año 2012 se reportaron numerosos ataques informáticos a través de malware como el dorkbot, que se propaga utilizando como pretexto noticias de interés general y coyuntural, tal es el de la agonía de Hugo Chávez.

almacenamiento), Colombia ostenta el tercer lugar con un 7%, Brasil ocupa el primer puesto con el 36% y México con el 34%[6].

Otro de los datos relevantes en lo que respecta a la seguridad de la información en América Latina en el año 2012, corresponde al primer caso espionaje industrial denominado "operación madre"[7], gusano ACAD/Medre. A, que afecta a archivos realizados con el programa de edición autocad, permitiendo el robo de diseños y planos en el ámbito industrial, que después son enviadas a cuentas de correo electrónico a China.

Los datos anteriormente señalados, indican el riesgo aparente en el que se encuentra Colombia con respecto a otros países de Latinoamérica y la importancia por tanto que debe otorgarse a un sistema de gestión de seguridad de la información -en especial en las empresas-, pues de este modo se podría contribuir a disminuir y evitar riesgos.

En este sentido, ISO elaboro la norma 27001 que estructura el sistema de seguridad de la información para las empresas, sistema que a partir de una serie de procesos y procedimientos genera el aseguramiento de la información de bajo, medio y alto riesgo.

Reconociendo la importancia de los sistemas de información en las empresas y organizaciones, se hace necesario que en las dinámicas de hoy se inicie el establecimiento de la norma ISO 27001, que no siendo la única forma de generar sistemas de seguridad de la información, si es la más utilizada en el ámbito colombiano; por ello cada vez más las empresas requieren y necesitan preparar sus sistemas para la implementación de la norma y de esta forma minimizar los riesgos a ataques y robos de la información.

[6]Información recuperada de http://latam.kaspersky.com/LatAmQ3malware2012 junior de 2013.
[7]Información recuperada de http://blogs.eset-la.com/laboratorio/wp content/uploads/2012/12/Infograf%C3%ACa-grande-acontecimientos-inform%C3%A1ticos-2012.jpg junio de 2013.

Por otro lado, en lo que respecta a La empresa., muestra de la presente investigación, el proyecto se justifica, toda vez que la empresa adquiere cada vez nuevos clientes de mayor envergadura, tanto en el sector privado como en el público, que hacen exigencias sobre la administración y seguridad de la información, pues ellos cumplen varias de la leyes y normatividad relacionadas con la seguridad de la información, generando que la empresa deba responder a dichos procesos.

Igualmente, la participación permanente en licitaciones públicas, en cuyas instancias la solicitud de un sistema de gestión de seguridad de la información es elemento indispensable para el cumplimiento de requisitos que exigen dichas licitaciones

El crecimiento del personal, infraestructura y arquitectura tecnológica hace indispensable un sistema de gestión de la información, que permita una administración acorde a las nuevas necesidades de ampliación de la empresa y de requerimientos de los nuevos clientes.

Por último el deseo de certificarse en ISO 27000 como una meta a mediano plazo, por parte de la gerencia de la empresa, reconoce la necesidad de implementar la metodología planteada en la presente investigación que contribuya significativamente al cumplimiento de dicha meta.

4. OBJETIVOS

4.1. OBJETIVO GENERAL

Aplicar las metodologías de generación de política y de gestión de riesgos en seguridad de la información, a través de un piloto en la empresa, para validarlas y realizar los ajustes necesarios en las mismas.

4.2. OBJETIVO ESPECÍFICO

a. Realizar un diagnóstico de seguridad de la información en la empresa. a partir de la aplicación de instrumentos de medición, tal como encuestas, para conocer su estado en seguridad de la información.

b. Aplicar la metodología de generación de política en seguridad de la información, a través de diferentes procesos y procedimientos en la empresa, para validarla y realizar los ajustes necesarios.

c. Aplicar la metodología de gestión de riesgos en seguridad de la información, en la empresa, incluyendo el estudio y la elección de una metodología acorde al contexto organizacional, para validarla y realizar los ajustes necesarios.

d. Evaluar los resultados de la aplicación de las metodologías realizando nuevamente la medición de la seguridad de la información en la empresa.

5. MARCO REFERENCIAL

5.1. ESTADO DEL ARTE

5.1.1. Tendencias actuales de seguridad informática

El estudio realizado por Andrés Ricardo Almanza Junco, CISO-Coordinador XIIJNSI, a partir de la XII Encuesta de Seguridad Informática realizada a 152 personas procedentes de los diferentes sectores productivos del país, arroja algunos elementos importantes relacionados no solo con la seguridad informática, sino igualmente con la seguridad de la información. La encuesta y su análisis presentan un panorama general sobre Colombia sus tendencias y limitaciones con respecto al tema de la seguridad informática y de la información.

Entre los resultados más importantes de la encuesta, se pueden observar los siguientes:

- No existe una directriz formal en los temas de seguridad de la información, dadas las nuevas amenazas tecnológicas y el avance de estas.
- Existe una creciente dependencia de la seguridad de la información con el área de tecnología, hecho que representa la manera como las empresas emprenden la seguridad de la información en primera instancia.
- La seguridad de la información cada vez cobra mayor importancia en las empresas, convirtiéndose en elemento prioritario en las agendas de trabajo de la Alta Dirección y dentro de las funciones más importantes de los altos cargos.
- El reconocimiento del capital humano de las empresas, sobre la importancia de la seguridad de la información es cada vez mayor, haciendo de esta parte indispensable de la cultura organizacional.

- Se evidencia una inversión de recursos en las empresas en lo que respecta a la seguridad de la información, en los aspectos de la creación de una política de seguridad de la información, y la conciencia de la seguridad y la protección de los datos en la nube.
- Otro elemento de inversión de las empresas en lo que respecta a la seguridad de la información, tiene que ver con la ciencia y el entrenamiento en seguridad, permitiendo asegurar el compromiso de los usuarios en el ciclo vital de seguridad de la información.
- En lo que se refiere a monitoreo permanente y continuo se ha mejorado significativamente en las empresas, pudiendo estas identificar eficazmente los incidentes y detectando mucho mejor las amenazas electrónicas.
- Otros de los aspectos en los que la seguridad de la información ha evolucionad significativamente, tiene que ver con las notificaciones de los colaboradores, la revisión de los logs[8] y la notificación de terceras partes, generando la comunicación de las fallas por parte de los miembros de la organización.
- Los grupos encargados de atención a los incidentes muestran un aumento significativo en las empresas, toda vez que se comprende la importancia y el riesgo de la protección de la información[9].

Estos son algunos de los resultados más significativos en lo que se refiere a la seguridad de la información, en la gran encuesta anual que al respecto realiza CISO, situación que demuestra el gran interés de las empresas colombianas por generar procesos al interior de las organizaciones que permitan crear un sistema de la seguridad de la información, que reduzcan los riesgos y dificultades en el tema.

Estas tendencias demuestran la prioridad que cada vez más va teniendo establecer metodologías para la implementación de sistemas de información

[8] Registros detallados de todos los movimientos y acceso al sistema.
[9] ALMANZA JUNCO, Andrés Ricardo. "seguridad informática en Colombia. Tendencias 2011-2012" en Revista sistemas seguridad y privacidad y sistemas de información. No. 123 abril-junio de 2012. ISSN 0120-5919. Bogotá. Colombia

confiables y seguros, razón por la cual es oportuno continuar aportando en este aspecto.

5.1.2. Sistemas de información y el sistema de gestión de seguridad de la información

Es fundamental iniciar reconociendo la diferencia entre un sistema de información y un sistema de gestión de seguridad de la información, pues de allí se deriva la intencionalidad de la presente investigación.

El sistema de información se refiere al almacenamiento, proceso, comunicación, entrada y salida de la información. "Sobre estas funciones elementales y a través del sistema operativo y las aplicaciones, se mantiene la información, se envían los mensajes y se ofrecen los servicios con valor para la organización"[10]

De otro lado el sistema de gestión de seguridad de la información se refiere: "entendida como el proceso o conjunto de actividades que permiten recopilar, clasificar, almacenar, asegurar, controlar, divulgar, apropiar, mantener y entender la información existente y producida por la empresa, tanto a nivel interno como externo."[11]

De este modo el sistema de la información debe ir acompañado de un sistema de gestión, ya que este permite el aseguramiento de la información que se maneja al interior de las empresas y la forma de procedencia de la misma.

El sistema de gestión de seguridad de la información fundamentalmente pretende asegurar buenas prácticas en el manejo y uso de la información, fomentar una cultura, cuidado y protección de la información y permitir que el capital humano de la empresa no se convierta en el principal foco de riesgo del manejo de la misma.

[10] ACEITUNO CANAL, Vicente "Seguridad de la Información: expectativas, riesgos y técnicas de protección" Op.Ed Noriega Editores. México. D.F. 2006

[11] ORTÍZ ANDRADE, Marcela. "Gestión de la información" en Revista Sistemas Inteligencia de Negocios. No. 120 julio-septiembre de 2010. ISSN 0120-5919.Bogotá. Colombia.

Las normas establecidas por ICONTEC, han generado procesos de gestión en diferentes ámbitos de la empresa, haciendo de estos espacios en los que la calidad de los servicios y productos ofrecidos sea el objetivo prioritario,

La norma ISO 9000 (conjunto de normas sobre calidad y gestión continua de la calidad)y 9001(requisitos para un buen sistema de gestión de la calidad) específicamente ofrecen la normatividad para implementar los SGC (Sistema de Gestión de la Calidad) en cualquier empresa, con un enfoque basado en procesos, que evidencie la mejora continua y las respectivas acciones correctivas y preventivas para satisfacer las necesidades del cliente.

Las empresas que han optado en la última década para certificarse en calidad con dichas normas, han olvidado que entre el ejercicio de calidad, se encuentra la protección y aseguramiento de la información que cotidianamente manejan los miembros de la empresa; por eso ISO establece una normatividad para generar un Sistema de Gestión de Seguridad de la Información

5.1.3. La Norma ISO 27001

La norma ISO 27001 publicada en 2005, el comité técnico de normalización 181 Técnicas de Seguridad de la información del ICONTEC, emprende la labor de adoptar la norma ISO 27001 como una norma nacional y en el mes de marzo de 2006 es ratificada como la NTC-ISO/IEC 2007[12]

[12] CALDER, Alan. "Nueve claves para el éxito. Una visión general de la implementación de la norma NTC-ISO/IEC 27001". ICONTEC. Governance publishing. Bogotá, Colombia. 2006

5.1.4. Antecedentes de la norma

El origen de la norma ISO 27001 es la norma BS7799 del Reino Unido que apareció en 1995, dicha norma al inicio era un código de práctica con respecto a la Gestión de la seguridad TI.

Este código se fue actualizando al paso del tiempo y realizando las mejoras necesarias, solo como documento de orientación y recomendación, pero en diciembre de 2000 se convierte con el criterio de norma solo para el Reino Unido, hasta que en 2005 adquiere el carácter internacional y se transforma en la ISO 27001.

5.1.5. Riesgos de la información

Una de las prioridades para la aplicación e implementación de las normas es iniciar el proceso haciendo ver a la organización la importancia de tener en la empresa un sistema de gestión de seguridad de la Información, pues aunque para muchos no sea importante, la norma desde un inicio tiene como propósito: "reducir y controlar los riesgos para la seguridad de la información. Por consiguiente la organización debe comprender, de la manera más cruda posible, que tales riesgos existen en relación con sus propias operaciones"[13]

De tal forma, las empresas deben comprender los diferentes riesgos y amenazas que puede tener la información almacenada en la organización y de allí establecer el ambiente necesario para gestar un sistema de gestión de la información, la aplicabilidad de la norma y si es posible finalizar con la certificación.

Para establecer un sistema de gestión de seguridad de la información, es importante tener en cuenta los siguientes elementos básicos de la norma ISO 27001

[13]Ibid, pág 15

1. Política de seguridad de la información
2. Organización de seguridad de la información. (Organización interna)
3. Organización de seguridad de la información. (Organización externa)
4. Gestión de activos
5. Responsabilidad por los activos
6. Clasificación de la información
7. Seguridad de los recursos humanos
8. Seguridad física del entorno
9. Gestión de comunicación y operaciones
10. Control de acceso
11. Adquisición, desarrollo y mantenimiento de sistema de información
12. Gestión de los incidentes de la seguridad de la información
13. Cumplimiento

Los anteriores corresponden a los requerimientos básicos de la norma y su implementación puede ser eficaz si se tiene en cuenta especialmente el recurso humano como elemento prioritario en la estructura del Sistema de gestión de seguridad de la información.

5.2. LA EMPRESA

5.2.1. Misión

Somos una empresa orientada a establecer relaciones de negocios de largo plazo, con base en escuchar las necesidades de nuestros clientes, permitiéndoles cumplir sus objetivos mediante la utilización de soluciones tecnológicas en Teleinformática, desarrolladas por nuestro equipo de trabajo.

Estamos comprometidos en hacer de nuestros productos las soluciones acertadas para las necesidades del mercado Latinoamericano, aspirando a ser líderes en el

segmento de mercado elegido, garantizando el desarrollo constante de la empresa y de cada uno de sus colaboradores.

5.2.2. Visión

Ser reconocidos en Latinoamérica para el año 2020 como el mejor socio de negocios para el desarrollo de soluciones tecnológicas en el sector de la Teleinformática, mediante la innovación, el mejoramiento continuo y la aplicación de estándares de calidad, aceptados internacionalmente.

5.2.3. Reseña Histórica

la empresa es una compañía especializada en el desarrollo de soluciones de software para computer telephony y comunicaciones, fundada el 09 de Junio de 1998 por un equipo de inversionistas del sector real e ingenieros socios gestores, con más de 13 años de experiencia en el área de las telecomunicaciones. La formación de la compañía coincidió con una de las épocas económicas más difíciles del país y la de región, sin embargo, el segmento de las telecomunicaciones ofrecía unas perspectivas de crecimiento interesantes, siempre y cuando se cumplieran con dos objetivos primordiales, el primero ofrecer soluciones de precio competitivo acorde a una economía con problemas en todos los países latinoamericanos y segundo, soluciones desarrolladas en Latinoamérica para Latinoamérica; ya que los productos existentes en el mercado son concebidos para infraestructuras y necesidades diferentes a las nuestras.

Consciente de la importancia de desarrollar productos de calidad la compañía enfoca su estrategia en establecer un plan fundamentado en su principal fortaleza, el desarrollo de soluciones, es por ello que renuncia a implementar una estructura comercial y opta por establecer alianzas con Resellers que le permitan ofrecer su

producto sin desenfocar su objetivo principal, es por ello que en Latinoamérica la empresa cuenta con BussinessPartner de la talla de Siemens, Alcatel, Nec, y Telenorma y cuenta con un portafolio de 8 soluciones, implementadas y probadas en más de 800 clientes en toda la región.

Una Trayectoria de Éxitos.

La Experiencia de nuestra compañía nos ha permitido méritos importantes y logros como los casos de éxito listados a continuación:

1. Primer Solución Colombiana con Señalización SS7 para Correo de Voz y Fax Públicos a más de 40.000 usuarios en la Ciudad de Barranquilla.

2. Primer Contact Center con Marcación Predictiva y CTI desarrollado en Latinoamérica con 300 agentes.

3. Primer Contact Center (Marcación Predictiva, Mensajería Unificada, Web Ennable, Total Logging, Fax Server, CTI y ACD) totalmente integrado a través de una Herramienta multiplataforma utilizando CSTA. LegisLec – Caracas Venezuela.

4. Primer Sistema de Correo de Voz corporativo para 3 sedes de la misma compañía integrada a través de AMIS recibiendo más de 750.000 llamadas mes. En diversos bancos del país.

5. Desarrollo Aplicación Especializada para CDC Centro de Comunicaciones en varias empresas.

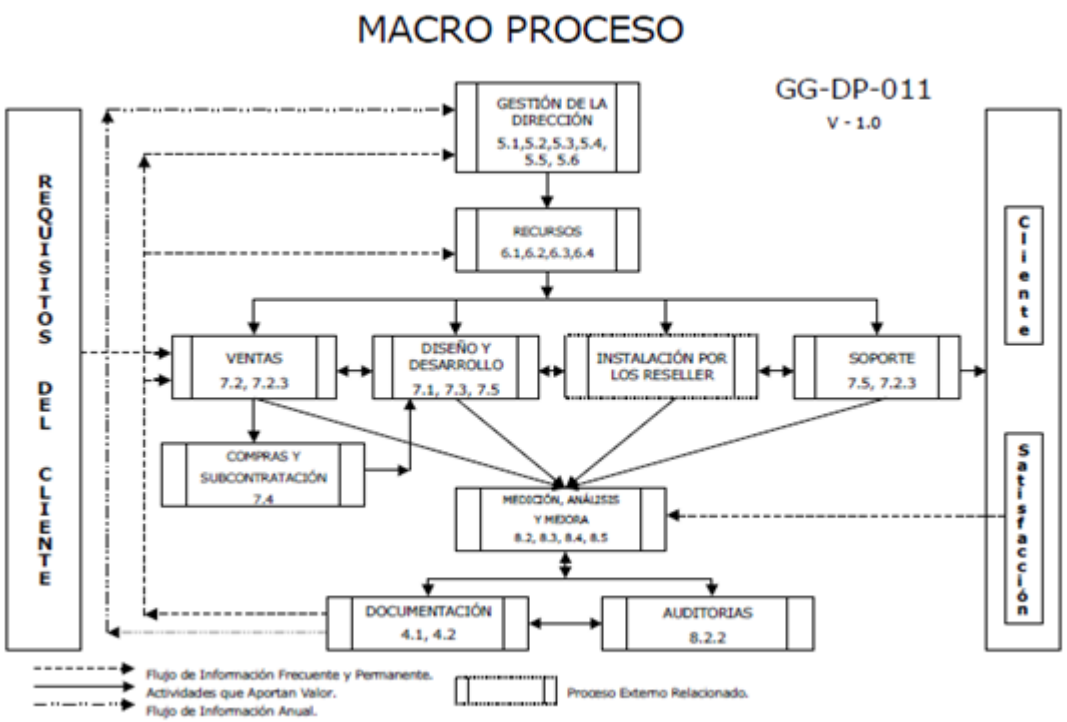
6. Especialización de Sistemas de Atención y Servicio al Cliente para entidades de Servicios Públicos.

7. Primer Sistema Digital de grabación de llamadas en extensiones propietarias, desarrollado en Latinoamérica.

8. Sistema de información de la gestión telefónica - Tarificador más de 600 en 3 años. Colombia, Venezuela, Ecuador y México.

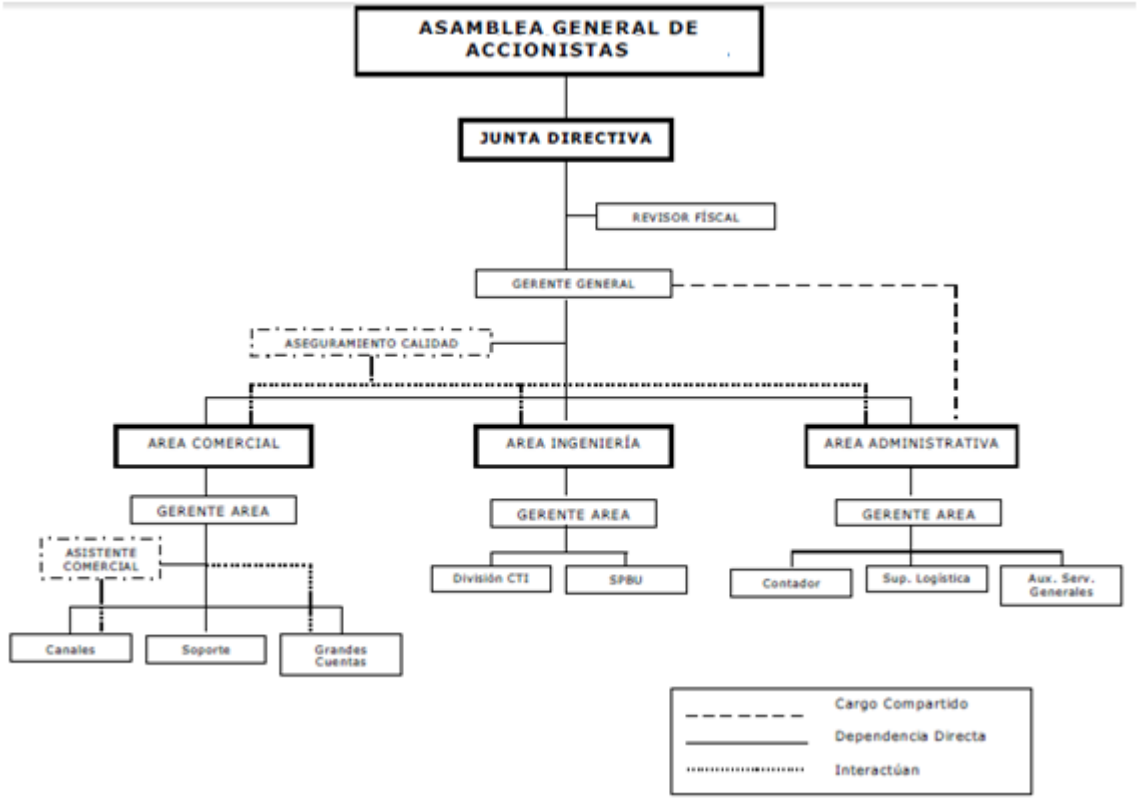
5.2.4. Mapa de procesos

Grafico 1: Mapa de procesos



Fuente. Manual de Calidad la empresa.

Grafico 2: Organigrama



Fuente. Manual de Calidad La empresa

5.2.5. Política de calidad

Quienes trabajamos en la empresa de teleinformática aseguramos que la calidad de nuestros productos y servicios satisfacen las necesidades de nuestros clientes. Nos comprometemos en hacer del sistema de calidad parte integral de nuestro trabajo garantizando el continuo mejoramiento de la organización y crecimiento de cada uno de sus integrantes personal y profesionalmente. Garantizamos con la

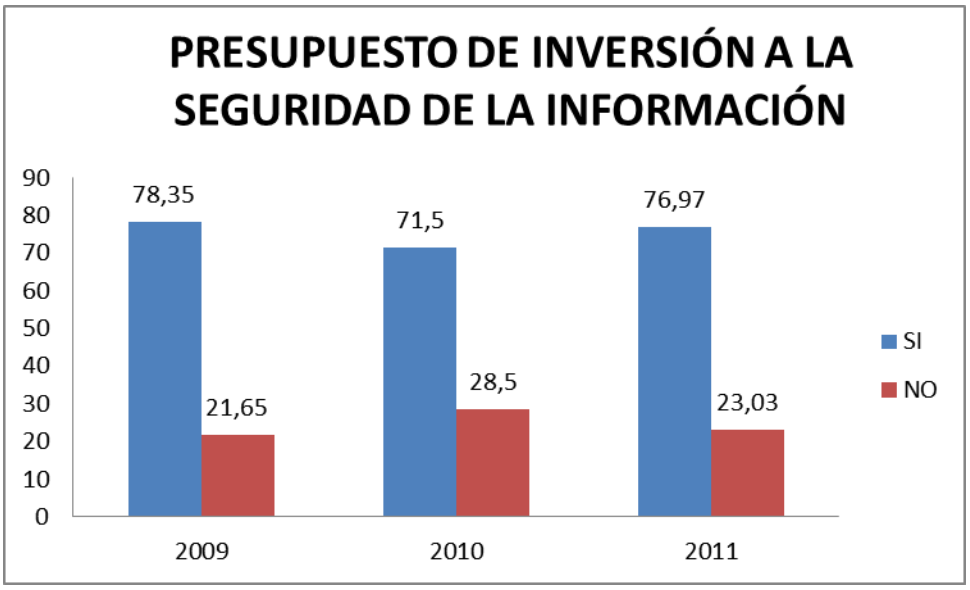
aplicación del Sistema de Calidad que el servicio al cliente es siempre exceder las expectativas del mismo. Aseguramos que nuestras soluciones de software cumplen con los requerimientos y especificaciones técnicas acordadas con los clientes. La medición del sistema de Calidad evalúa el cumplimiento de los objetivos de Calidad a través de índices de gestión.

5.3. MARCO DE ANTECEDENTES

5.3.1. Ámbito nacional

Es importante en principio reconocer como se encuentra el país en lo que respecta a la seguridad de la información, esto para establecer la situación particular de La empresa., con respecto al ámbito nacional y así instaurar comparaciones que aborden el problema de investigación de manera más acertada.

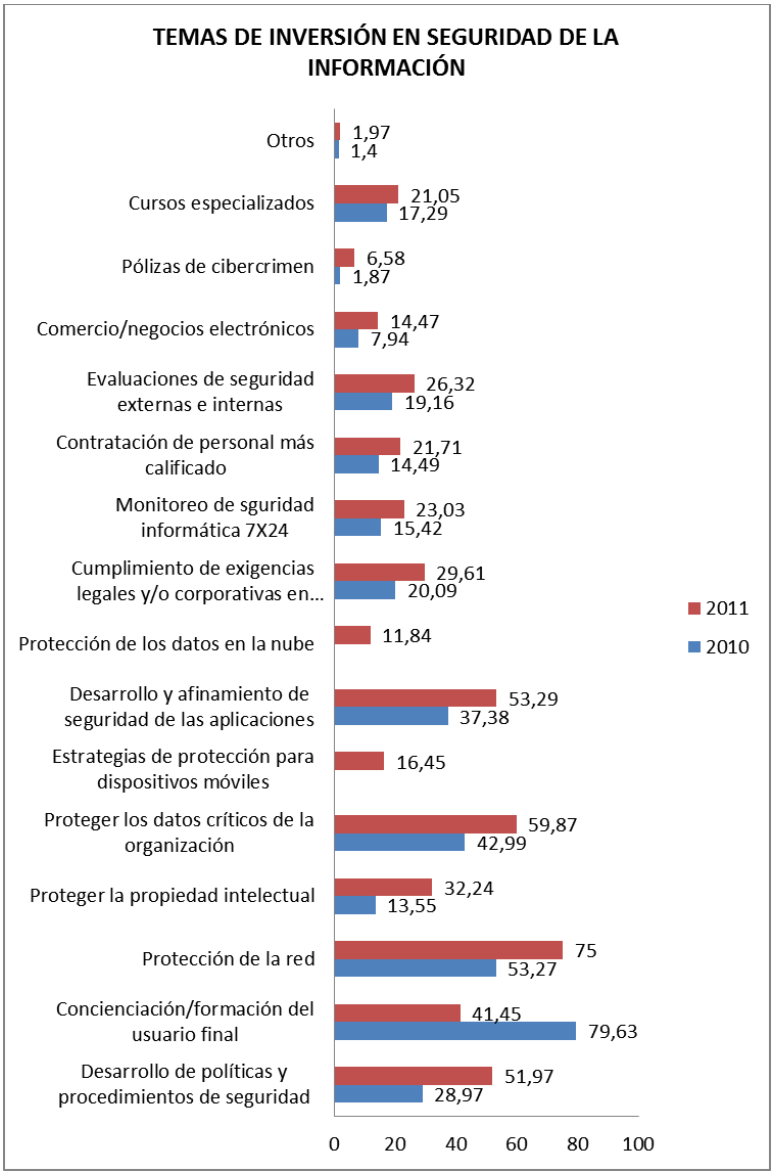
Grafico 3: Presupuesto de Inversión a la seguridad de la información



Fuente: Encuesta Seguridad de la Información en Colombia tendencias 2011-2012

Se observa un crecimiento significativo en el presupuesto destinado a la seguridad de la Información, teniendo en cuenta que cada vez más las empresas toman conciencia de la importancia de proteger y salvaguardar todo lo relacionado con la información y el significado en detrimento del capital que significa un robo o incidente en el tema.

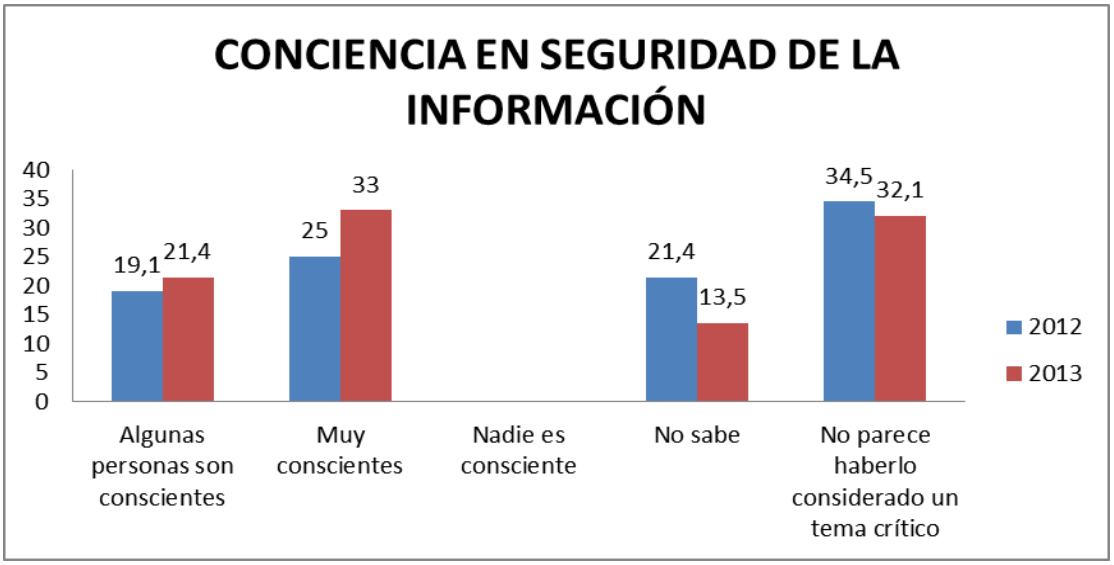
Grafico 4: Temas de Inversión en Seguridad de la Información



Fuente: Encuesta Seguridad de la Información en Colombia tendencias 2011-2012

Se evidencia fundamentalmente la protección de las redes y de datos críticos en las redes; especialmente se observa un crecimiento en lo que respecta a la inversión para la creación de políticas de seguridad, situación que demuestra la importancia de la generación de metodologías que apunten específicamente a este campo, tomando así relevancia el presente proyecto de investigación.

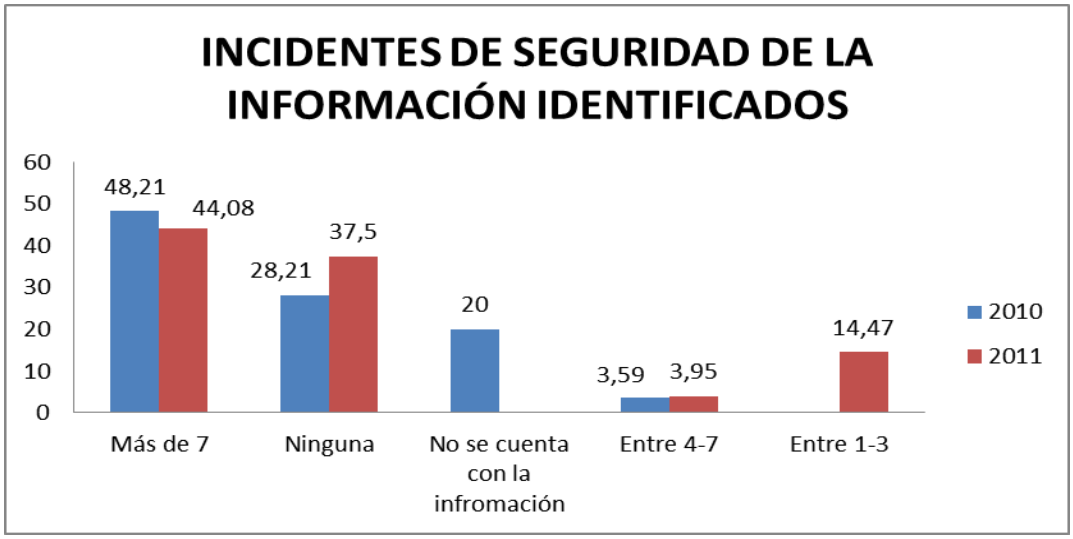
Grafico 5: Conciencia en seguridad de la Información



Fuente: Encuesta Seguridad de la Información en Colombia tendencias 2011-2012

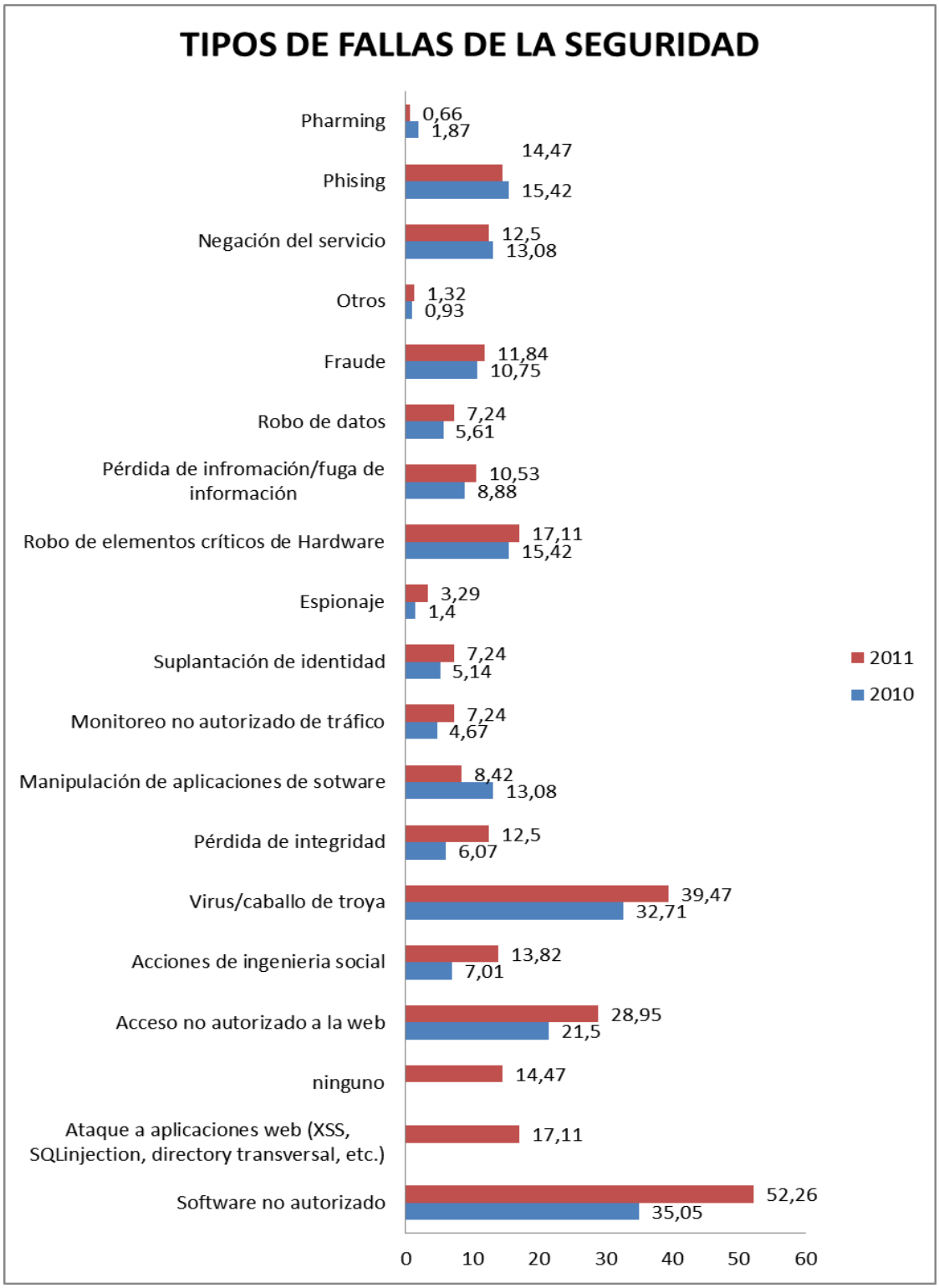
La mayoría de los miembros de la organización son conscientes de la importancia de implementar sistemas que optimicen los procesos de seguridad de la información; toda vez que estos disminuyen riesgo y previenes situaciones críticas; Con el paso del tiempo y el vertiginoso avance de las tecnologías los miembros de las organizaciones consideran con mayor atención los asuntos relacionados con la seguridad de la información y esperan obtener mejores resultados al implementar sistemas de gestión.

Grafico 6: Incidentes de Seguridad de la Información Identificados



Fuente: Encuesta Seguridad de la Información en Colombia tendencias 2011-2012

Grafico 7: Tipos de Fallas



Fuente: Encuesta Seguridad de la Información en Colombia tendencias 2011-2012

Teniendo en cuenta los dos gráficos anteriores, es importante resaltar que aumenta el número de incidentes en las organizaciones; al igual que el establecimiento de indicadores para determinar el tipo de incidentes asociados a la seguridad de la información, en el que se destaca los virus, los software no autorizados, robo de elementos críticos de Hardware; situación que demuestra las condiciones de mayor riesgo dentro de las empresas y que deben ser significativas en la intención de generar sistemas de seguridad de la información.

El anterior panorama, indica como en Colombia se hace necesaria cada vez más la implementación de Sistemas de Seguridad de la Información, que minimicen los riesgos e incidentes, de esta forma prevenir futuros ataques a la información de las empresas, permitiendo que optimice el valor y sentido de las organizaciones.

5.3.2. Ámbito de la empresa.

En lo que respecta a la empresa, muestra de la presente investigación, en lo que se refiere a la seguridad de la información es importante destacar como antecedentes los siguientes:

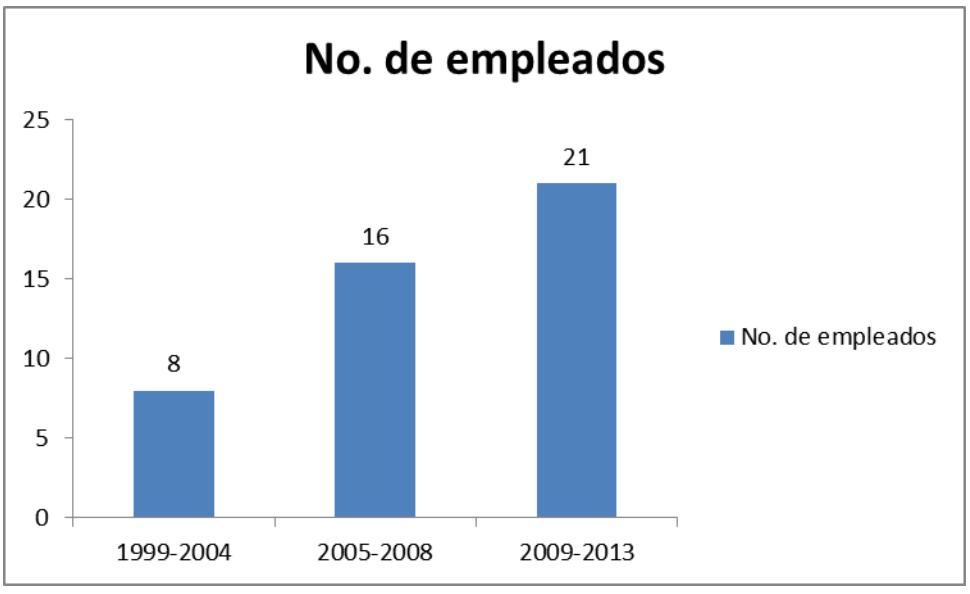
A la fecha la empresa no cuenta con una política de seguridad, ni existe un equipo o dependencia encargada de esta área, lo que refiere a situaciones o exigencias al respecto solicitada por clientes interno o externos es llevada por cualquier miembro de la organización, que cuente con cierta experiencia o posea el tiempo para cumplir con los requerimientos.

A partir de un estudio desarrollado en la empresa, se observa la necesidad creciente de contar con un Sistema De Gestión De Seguridad De La Información, que permita minimizar riesgos, debido entre otras situaciones al crecimiento de la empresa.

Grafico 8**:** Clientes Externos

Fuente: información de los archivos de la empresa.

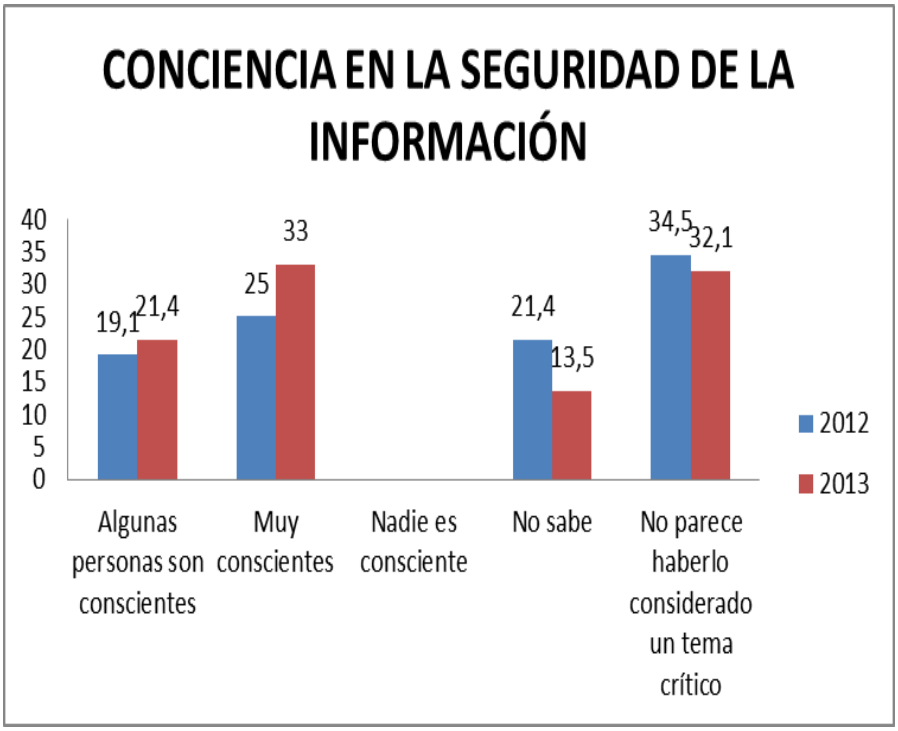
Grafico 9: Número de Empleados



Fuente: información de los archivos de la empresa.

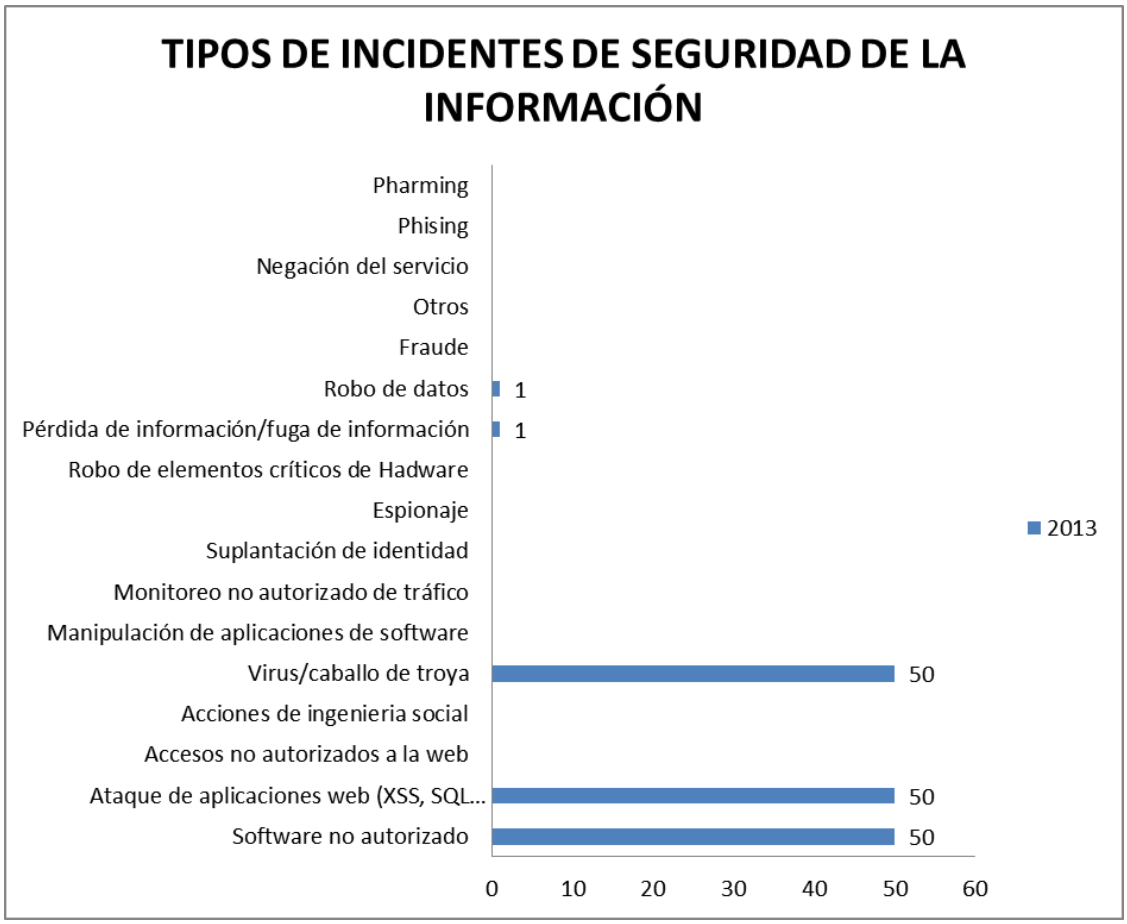
Durante el más reciente periodo de tiempo la empresa ha iniciado un proceso de crecimiento y expansión tanto en su personal, como en lo que respecta a los clientes externos, situación que exige ser cada vez más cuidadoso y severo con el manejo de la información; la solicitud de los clientes externos de contar con ciertos requerimientos asociados a la legislación y normatividad de la seguridad de la información, motiva a la empresa de abordar un SGSI.

Gráfico 10: Conciencia en la Seguridad de la Información



Fuente: información de los archivos de la empresa

Grafico 10: Tipos de Incidentes de Seguridad de la Información



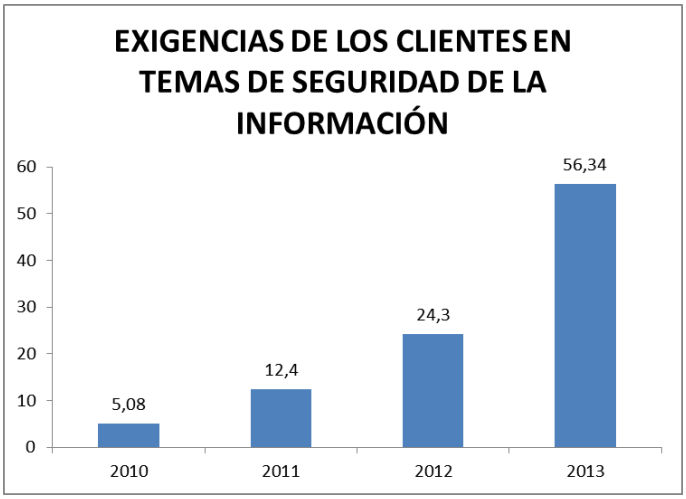
Fuente: información de los archivos de la empresa

Por otro lado, los anteriores gráficos representan la situación de la empresa en estudio con respecto a la seguridad en la información, en la que se destaca entre otros aspectos, una creciente concienciación con respecto a proteger y asegurar la información, esto debido a las exigencias del mundo empresarial y las dinámicas propias de la globalización.

En este mismo sentido, otra de las razones es el aumento en incidentes de seguridad de la información entre las que se destacan ataques de virus y software no autorizados y ataques a las aplicaciones y un incidente delicado de robo de información de un código fuente pionero de la empresa, por parte de uno de los miembros de la organización, que al ser hurtado le permitió a dicha persona constituir su propia empresa y convertirla en competencia de la empresa.

En este mismo sentido, ante los incidentes de seguridad de la información, la empresa no cuenta con una política claramente definida, que permita evitar otros incidentes como los anteriormente señalados, igualmente no hay metodología de riesgos o controles al respecto; lo que hace indispensable iniciar un proceso para establecer el SGSI, o por lo menos los criterios iniciales para instituirlo. Aunque algunos clientes externos exigen en las licitaciones públicas una política de seguridad esta se diseña para responder a los requerimientos específicos, pero esta no es socializada y mucho menos aplicada.

Grafico 11: Exigencia de los Clientes en Temas de Seguridad de la Información



Fuente: información de los archivos de la empresa

De la misma manera, ante el aumento de licitaciones y clientes, la empresa entiende la importancia de generar las condiciones iniciales para dar paso a la construcción de una política de seguridad que más allá de atender un

requerimiento legal, sea la política que minimice riesgos y prevenga incidentes; ya que en el sector público y privado son más altas las exigencias de seguridad de la información, situación que la empresa estudio tiene en cuenta pues como se señala en la gráfica anterior el aumento en dichos requerimientos paso de un 24.3% en el 2012 a un 56,34% en el 213.

5.4. MARCO CONCEPTUAL

5.4.1. Seguridad de la información

Son todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información. El concepto de Seguridad de la Información no debe ser confundido con el de Seguridad Informática, ya que este último solo se encarga de la seguridad en el medio informático, pudiendo encontrar información en diversos medios o formas[14].

5.4.2. Seguridad informática

Seguridad Informática es el proceso de prevenir y detectar el uso no autorizado de las computadoras. “La Seguridad Informática es un proceso continuo, donde la condición de los controles de la institución es apenas un indicador de su postura de seguridad”[15].

[14]Recuperado de http://seguridadinformatica.unad.edu.co/index.php/seguridad junio de 2013
[15]FFIEC Information Security IT Examination Handbook, Diciembre de 2002.

5.4.3. Sistema Gestión de Seguridad de la Información (SGSI)

El Sistema de Gestión de Seguridad de la información (SGSI) se basa en la norma ISO/IEC 27001:2005 - establecida por la organización internacional de estándares ISO -, específicamente en los aspectos y mejores prácticas que las organizaciones deben tener para tratar los temas de seguridad de la información. La norma específica 5 requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información en la organización (SGSI), además de una serie de controles y objetivos de control, divididos en 11 dominios, que se han encontrado pertinentes en las organizaciones y de los cuales se debe especificar los que serán seleccionados como parte del proceso del SGSIR[16]

5.4.4. ISO

Es una organización internacional de normalización, con sede en Ginebra Suiza. Es una agrupación de organizaciones nacionales de normalización, cuyo objetivo es establecer, promocionar y gestionar estándares.[17]

La ISO surge el 23 de febrero del año 1947 publicando a la fecha de hoy 16500 normas internacionales, siendo las relacionadas con las tecnologías de la información las normas más recientes publicadas.

5.4.5. ISO 27000

Una familia de estándares internacionales para sistemas de gestión de la seguridad de la información, cubre todos los tipos de organizaciones y en esta se proponen los siguientes requerimientos:

[16]Recuperado de http://sgsi.utp.edu.co/ julio de 2013

[17]Recuperado de http://www.iso27000.es/glosario.html#section10i junio de 2013

*Requisitos para la especificación de sistemas de gestión de seguridad de la información.

*Proceso del análisis y gestión del riesgo

*Métricas y medidas de protección

*Guías de implantación.

*Vocabulario claramente definido para evitar diversas interpretaciones de conceptos técnicos de gestión y de los procesos de mejora.

5.4.6. Política de seguridad

Las políticas de seguridad son documentos definidos por los responsables directos o indirectos de un sistema, se constituye en la base del entorno de seguridad de una empresa y deben definir las responsabilidades, los requisitos de seguridad, las funciones, y las normas a seguir por los trabajadores de la misma.[18]

5.4.7. Metodología

Es una guía que nos indica que hacer y cómo actuar para alcanzar los objetivos propuestos en una investigación.

5.4.8. Evaluación del riesgo

La gestión del riesgo contempla el “cálculo del riesgo, la apreciación de su impacto en el negocio y la posibilidad de ocurrencia”.

[18] Recuperado de http://mmc.geofisica.unam.mx/LuCAS/Manuales-LuCAS/doc-unixsec/unixsec-html/node333.html julio del2013

La evaluación del riesgo identifican, cuantifican y priorizan los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra dichos riesgos[19].

5.4.9. Phishing

Es uno de los métodos más utilizados por delincuentes cibernéticos para estafar y obtener información confidencial de forma fraudulenta como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria de la víctima.

El estafador, conocido como phisher, se vale de técnicas de ingeniería social, haciéndose pasar por una persona o empresa de confianza en una aparente comunicación oficial electrónica, por lo general un correo electrónico, o algún sistema de mensajería instantánea, redes sociales SMS/MMS, a raíz de un malware o incluso utilizando también llamadas telefónicas.[20]

5.4.10. Pharming

Es la explotación de una vulnerabilidad en el software de los servidores DNS (Domain Name System) o en el de los equipos de los propios usuarios, que permite a un atacante redirigir un nombre de dominio (domainname) a otra máquina distinta. De esta forma, un usuario que introduzca un determinado

[19]Tecnologías de la Información-técnicas de seguridad-código para la práctica de la gestión de la seguridad de la información. Segunda edición. 2005.
[20]Recuperado de http://es.wikipedia.org/wiki/Pharming julio de 2013

nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado para ese nombre de dominio[21].

[21] Recuperado de http://forum.bitdefender.com/index.php?showtopic=14797 julio del 2013

6. DISEÑO METODOLÓGICO

6.1. HIPÓTESIS

La aplicación de las metodologías de generación de política y de gestión de riesgos mejorará la seguridad de la información en la empresa

6.2. ENFOQUE DE LA INVESTIGACIÓN

La investigación tiene un enfoque cuantitativo, toda vez que pretende implementar una metodología*: aplicación de las metodologías para la generación de política y para la gestión de riesgos en el marco del establecimiento del SGSI,* cuyo ejercicio se encuentra relacionado con la medición de resultados y su respectivo impacto.

El enfoque se justifica, ya que "la investigación cuantitativa se dedica a recoger, procesar y analizar datos cuantitativos o numéricos sobre variables previamente determinadas. Esto ya hace darle una connotación que va más allá de un mero listado de datos organizados como resultado; pues estos datos que se muestran en el informe final, están en total consonancia con las variables que se declararon desde el principio y los resultados obtenidos van a brindar una realidad específica a la que estos están sujetos".[22]

6.3. TIPO DE INVESTIGACIÓN

La investigación es de tipo exploratorio, ya que los estudios exploratorios sirven para familiarizarse con fenómenos relativamente desconocidos, obtener información sobre la probabilidad de llevar a cabo una investigación más compleja

[22] http://www.monografias.com/trabajos63/investigacion-cuantitativa/investigacion-cuantitativa.shtml

sobre el tema[23]; desde esta perspectiva la presente investigación pretende generar validez a un ejercicio investigativo anterior que diseña una variable a ser aplicada y que de dichos resultados puede surgir una nueva investigación o definir la anterior.

En este sentido, puede definirse como exploratoria, toda vez que pretende sumergirse en los ámbitos de validación y no en el diseño de la metodología.

6.4. METODOLOGÍA

Para el cumplimiento de los objetivos del presente proyecto de investigación se debe tener en cuenta la metodología planteada por el grupo de investigación Nyquist y siguiendo con las actividades, procedimientos y variables a continuación señaladas:

Objetivo 1: Realizar un diagnóstico de seguridad de la información en la empresa a partir de la aplicación de instrumentos de medición, tal como encuestas, para conocer su estado en seguridad de la información.

Para lograr este objetivo se establecerá la línea base de la seguridad de la información realizando una encuesta a los miembros de la empresa y revisando los procesos para conocer y diagnosticar la situación actual de los activos de información de la organización; así mismo se validará el cumplimiento de controles de seguridad.

Igualmente, se realizará una revisión exhaustiva de la documentación de la empresa y el Sistema Gestión de la Calidad para determinar y concluir la línea base de la seguridad de la información, determinando así las necesidades de protección de la información.

[23] HERNÁNDEZ SAMPIERI, R, FERNÁNDEZ COLLADO, C, BAPTISTA LUCIO, P. "Metodología de la investigación". McGraw-Hill. México D.F. cuarta edición. 2006. Pág.59

Objetivo 2: Aplicar la metodología de generación de política en seguridad de la información, a través de diferentes procesos y procedimientos en la empresa, para validarla y realizar los ajustes necesarios.

Para lograr este objetivo se aplicará la metodología definida por el grupo de investigación Nyquist, resultado de un proceso de investigación y se procederá a realizar los ajustes necesarios.

Objetivo 3: Aplicar la metodología de gestión de riesgos en seguridad de la información, en la empresa, incluyendo el estudio y la elección de una metodología acorde al contexto organizacional, para validarla y realizar los ajustes necesarios.

Para alcanzar este objetivo se estudiarán diferentes metodologías de gestión de riesgos y se procederá a seleccionar una para aplicar en la empresa. Una vez seleccionada la metodología, se realizará un ciclo de gestión de riesgos para validarla y se realizarán los ajustes necesarios.

Objetivo 4: Evaluar los resultados de la aplicación de las metodologías realizando nuevamente la medición de la seguridad de la información en la empresa.

Una vez aplicadas las metodologías de generación de política y de gestión de riesgos, se medirá nuevamente el estado de la seguridad de la información en la empresa, de la misma manera que se realizó en el objetivo 1, para verificar la mejora en la seguridad de la información y para la validación de la hipótesis.

6.5. POBLACIÓN Y MUESTRA

Como población se destacan las empresas del sector de soluciones tecnológicas en teleinformática en la ciudad de Bogotá D.C., como lo son Eagleware, PCSistel,

Abacoox, Nice, Werimp, Repbox, Rightfast, Sagem, MyFax entre otros, que en el sector se establecen como competencia directa de la empresa.,

Se puede considerar un segundo estudio de caso, ya que la validez de la metodología diseñada por el grupo Nyquist inicialmente se probará en una entidad pública de la ciudad de Pereira y posteriormente en una empresa localizada en la ciudad de Bogotá, cuya misión es la solución de comunicaciones, llamada la empresa., dicha empresa se encuentra certificada en calidad por la norma ISO 9001, y se constituirá en la muestra de la investigación.

En el momento no cuenta con un Sistema de Gestión de Seguridad de la Información, siendo importante tenerlo, pues por la naturaleza de la empresa se maneja información crítica y sensible, careciendo en gran parte de los medios para garantizar la protección de dicha información; en este sentido la empresa. se constituye en la muestra óptima para dar validez a la metodología y cumplir los objetivos investigativos.

7. EJECUCIÓN E IMPLEMENTACIÓN DEL PROYECTO DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA.

7.1. CAPITULO 1: DIAGNÓSTICO DE LA EMPRESA. EN SEGURIDAD DE LA INFORMACIÓN

En miras de obtener un diagnóstico verás en lo que respecta a seguridad de la información en la empresa, antes de la ejecución del presente proyecto, se aplicaron dos encuestas; una de ellas dirigidas a cada uno de los miembros de la empresa y a cada una de las áreas o dependencias de la organización y la otra al encargado de la seguridad de la información, toda vez que la empresa en la actualidad no tiene dispuesto un equipo para lo relacionado con el tema de seguridad, solo ha dispuesto a una persona para que maneje ciertos aspectos con relación a la seguridad de la información.

En la actualidad (año 2013) la empresa cuenta con 22 empleados distribuidos en tres áreas:

1. El ***área administrativa*** que se compone fundamentalmente de los siguientes miembros:

a. Asistente contable:
b. Asistente administrativo
c. Auxiliar de oficina
d. Jefe de aseguramiento de la calidad
e. Coordinador administrativo
f. Asistente de servicios generales
g. Gerente General

2. El ***área de Ingeniería*** que se compone fundamentalmente de los siguientes miembros:

a. Ingeniero de diseño de aplicaciones
b. Director de diseños de aplicaciones
c. Ingeniero de desarrollo de aplicaciones

d. Jefe de desarrollo de aplicaciones
e. Director de ingeniería
f. Director de ingeniería e investigación y desarrollo
g. Ingeniero Senior
h. Consultor de desarrollo de aplicaciones

3. El ***área comercial*** que se compone fundamentalmente de los siguientes miembros:

a. Gerente de cuenta
b. Director de canales
c. Marca especialista en comunicaciones
d. Ejecutivo de cuentas y asistente de marketing
e. Director de ventas y mercadeo

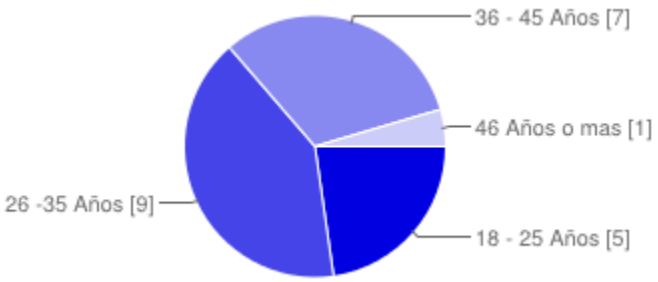
Todos ellos en ocupación de cumplir funciones relacionadas con el portafolio de la empresa.

Los resultados obtenidos en la encuesta aplicada a cada uno de los miembros (ver anexo 1), representan el estado actual en lo referente a la seguridad de la información y permitió evidenciar la situación de la empresa y la línea base para la aplicación de la metodología en la construcción de la política de seguridad de la información.

La caracterización de la población de la empresa permite evidenciar aspectos importantes para el desarrollo de la presente investigación, toda vez que representa posibilidades y necesidades en dicha empresa.

A continuación se presentan los resultados obtenidos con su respectivo análisis:

Grafico 12: Edad de los miembros de la empresa



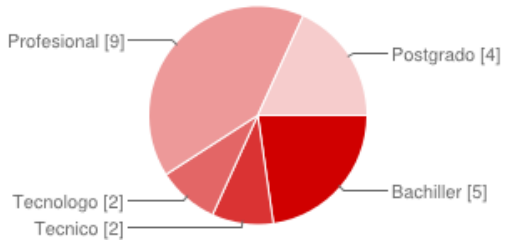
Respuesta	Encuestados	Porcentaje
18 - 25 Años	**5**	23%
26 -35 Años	**9**	41%
36 - 45 Años	**7**	32%
46 Años o mas	**1**	4%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

La empresa cuenta con un personal joven que no supera en su gran mayoría los 45 años, situación que puede beneficiar a la misma en la implementación de los Sistemas de Seguridad de la Información; ya que dicha población puede acceder más fácil a las nuevas tecnologías y significa quizás un acercamiento mayor a las mismas.

Grafico 13: Nivel de escolaridad



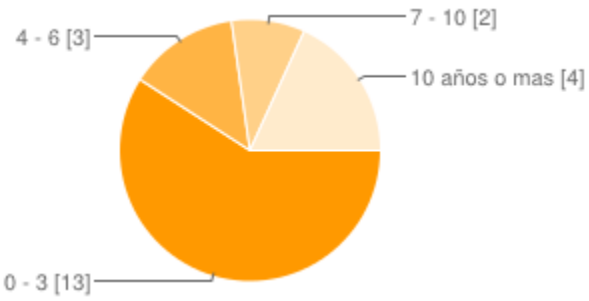
Respuesta	Encuestados	Porcentaje
Bachiller	**5**	23%
Técnico	**2**	9%
Tecnólogo	**2**	9%
Profesional	**9**	41%
Posgrado	**4**	18%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

En este mismo sentido, un gran porcentaje 41% de los miembros de la empresa son profesionales, situación que permite el reconocimiento de ciertos procesos y el liderazgo en la innovación y requerimientos propios del SGSI.

Grafico 14: Permanencia en la empresa



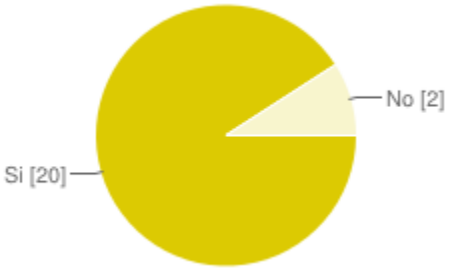
Respuesta	Encuestados	Porcentaje
0 - 3	**13**	59%
4 - 6	**3**	14%
7 - 10	**2**	9%
10 años o mas	**4**	18%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Por otro lado, se observa una inestabilidad laboral en la empresa; ya que un 59% de los miembros llevan laborando entre 0 y 3 años, esto debido quizás a lo relativamente joven de la empresa, pero esta inestabilidad puede ser un punto poco benéfico para la continuidad de los procesos y el liderazgo en la implementación de los SGSI.

Grafico 15: Conocimientos sobre seguridad de la información



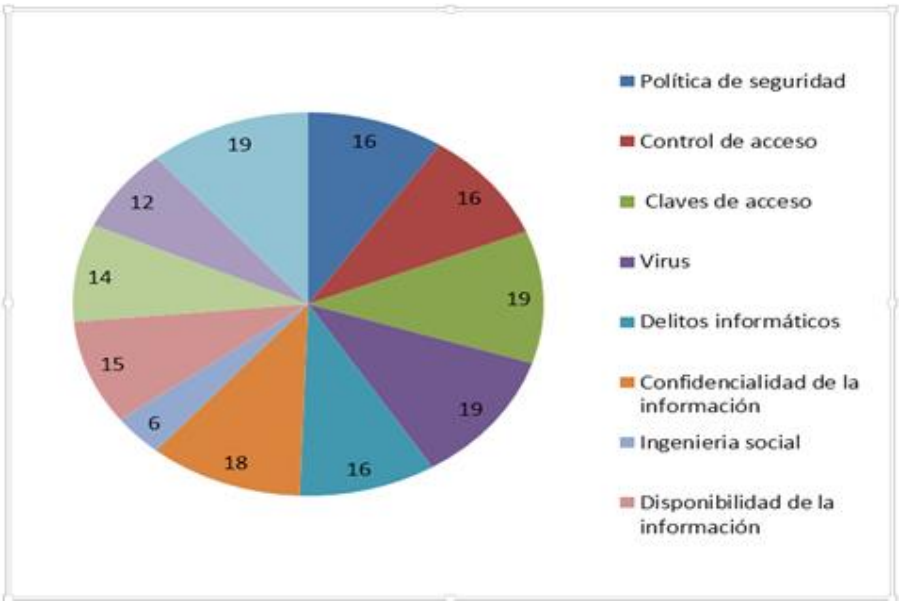
Respuesta	encuestados	Porcentaje
Si	**20**	91%
No	**2**	9%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Ante los conocimientos que poseen los miembros de la empresa en lo relativo a la Seguridad de la Información, es importante destacar que un alto porcentaje (91%) señala que si conoce qué es seguridad de la información, situación que al observar otros resultados en la encuesta permite evidenciar que dicho conocimiento es superficial y que no supera sino el saber sobre el cuidado que debe tenerse con respecto a todo tipo información que se maneja en el empresa.

Grafico 16: ¿Cuál de los siguientes términos conoce o maneja?



Pregunta	Encuestados No conocen	Porcentaje
Política de seguridad	**16**	72%
Control de acceso	**16**	72%
Claves de acceso	**19**	86%
Virus	**19**	86%
Delitos informáticos	**16**	72%
Confidencialidad de la información	**18**	81%
Ingeniería social	**6**	27%
Disponibilidad de la información	**15**	68%
Integridad de la información	**14**	63%
Autenticación de la información	**12**	54%
Confidencialidad de la información	**19**	86%

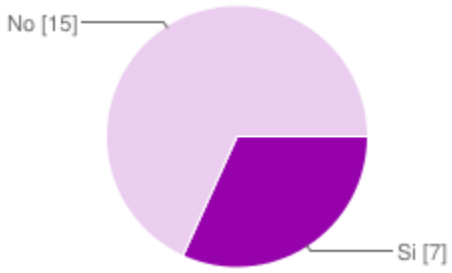
Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

La anterior gráfica, corresponde a preguntar a los miembros de la organización sobre sus conocimientos específicos acerca de la seguridad de la información, se señalan en la tabla y en el gráfico el número de personas que respondieron negativamente y su porcentaje del total de encuestados que fue de 22 personas,.

Al preguntarse a los encuestados sobre aspectos específicos de seguridad de la información, se corrobora lo anteriormente dicho, que el conocimiento sobre Seguridad de la Información obedece a un saber puramente superficial, lo relacionan resultados como, el manejo de pocos miembros de la empresa con términos que se relacionan estrechamente con la Seguridad de la Información y no permiten abordar la misma de forma compleja y significativa; desconocen qué es una política de seguridad de la información o autenticación de la información, estos elementos son de importancia y relevancia para definir que si existe un conocimiento sobre Seguridad de la Información por los miembros de la empresa; de tal modo, que al desconocerlos y mucho menos manejarlos, se puede afirmar que el conocimiento sobre Seguridad de la Información, es solo del término pero no de sus procesos, ventajas y demás.

Grafico 17: Capacitación sobre seguridad de la información

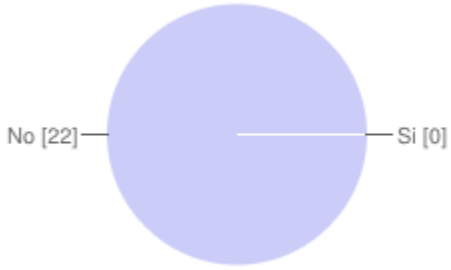


Respuesta	Encuestados	Porcentaje
Si	**7**	32%
No	**15**	68%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Grafico 18: Capacitación sobre seguridad de la información en la organización



Respuesta	Encuestados	Porcentaje
Si	**0**	0%
No	**22**	100%

Fuente: Autor

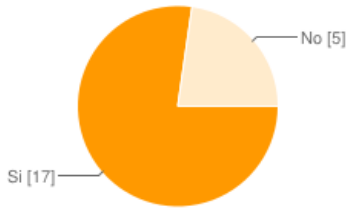
Referencia: Encuesta Seguridad de la Información (julio de 2013)

La empresa igualmente, no realiza las capacitaciones necesarias para los miembros de la comunidad, lo que se observa en los resultados pues 100% de los empleados afirman no haber recibido capacitación y solo el 32% de ellos recibió capacitación al respecto, pero en otro espacio diferente de la empresa.; en este sentido, la organización debe comprender la importancia de capacitar a todos los integrantes, pues con un porcentaje tan pequeños no es posible lograr los propósitos de la implementación de SGSI, teniendo en cuenta que los que han recibido capacitación sobre este tema ha sido de manera externa, y no dentro de la empresa, pues ella hasta el momento no ha considerado como prioridad capacitar y formar en lo relacionado con Seguridad de la Información, teniendo en cuenta que manejan información crítica, es importante asumir con prontitud este aspecto en la empresa.

Es importante denotar que siendo la empresa. una empresa con un porcentaje muy alto de miembros pertenecientes al campo de la administración y la

ingeniería en sistemas y relacionados, permite observar que son ellos los ingenieros precisamente los que más se acercan al tema de la Seguridad de la Información, debido a la formación profesional.

Grafico 19: Clave de acceso al sistema



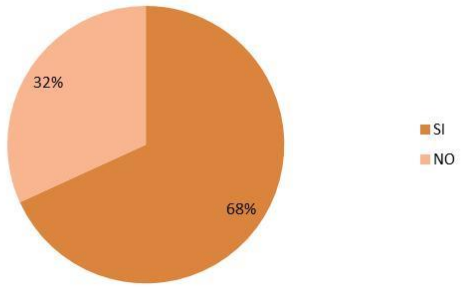
Respuesta	Encuestados	Porcentaje
Si	**17**	77%
No	**5**	23%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

De la misma forma, se observar que la empresa maneja en un gran porcentaje, el 77% de control en el acceso a los equipos y a la información que contienen, ya que cada funcionario de la empresa para acceder al sistema se debe hacer con una clave de usuario, situación que permite un grado de confidencialidad y seguridad en la información que se recibe y maneja desde dichos dispositivos; sin embargo aunque el porcentaje es alto, no es del 100%, por ello es necesario llegar al pleno funcionamiento de la seguridad de la información al respecto. En este mismo sentido, en lo que respecta a la seguridad de las contraseñas en los correos electrónicos solo el 68% posee una adecuada, para los requisitos de un Sistema de Seguridad de la Información.

Grafico 20: Seguridad de la contraseña del correo electrónico

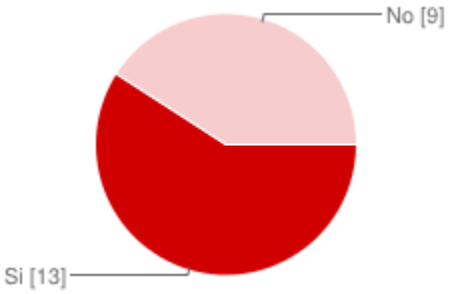


Respuesta	Encuestados	Porcentaje
Si	**15**	68%
No	**7**	32%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Grafico 21: Información sobre la confidencialidad de la información al ingresar a la empresa



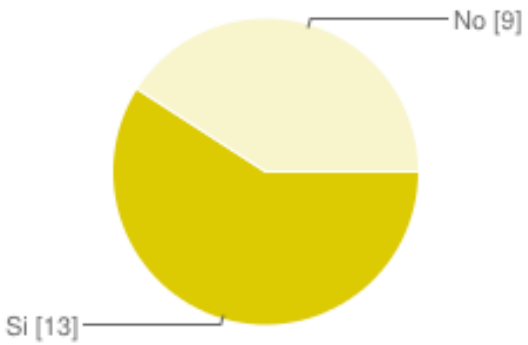
Respuesta	Encuestados	Porcentaje
Si	**13**	59%
No	**9**	41%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Por otro lado, es fundamental indicar que no todos los miembros de la organización se les comunica sobre la confidencialidad de la información al momento de ingresar a la organización; razón por la cual un 41% de los miembros no consideran importante el manejo de la información de forma segura y eficiente, pudiendo presentarse algún incidente en la seguridad de la información.

Grafico 22: Cláusulas de confidencialidad de la información en el contrato

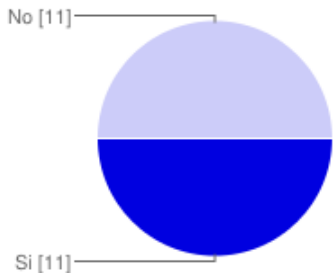


Respuesta	Encuestados	Porcentaje
Si	**13**	59%
No	**9**	41%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Grafico 23: Libre acceso a la información de la empresa



Respuesta	Encuestados	Porcentaje
Si	**11**	50%
No	**11**	50%

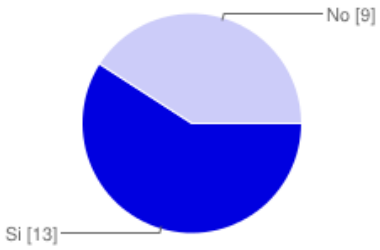
Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

De la misma forma, en el contrato laboral el 59% de los miembros recuerdan haber firmado clausulas relacionadas con el manejo y cuidado de la información, situación que es significativa, pero que de una u otra forma debe hacerse generalizada para todos los miembros, así no manejen información sensible.

Todo esto teniendo en cuenta que el 50% de los miembros de la organización goza de libre acceso a la información que se maneja en la empresa; esto permite observar que no se posee los requerimientos necesarios para asegurar la información e impedir que sucedan incidentes relacionados con el tema.

Grafico 24: Conocimiento sobre la autenticación de usuarios al ingreso de la información



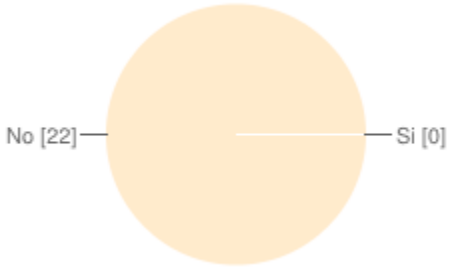
Respuesta	Encuestados	Porcentaje
Si	**13**	59%
No	**9**	41%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Igualmente, los miembros de la organización en un 59% conocen los procedimientos documentados relacionados con la autenticación de usuarios, situación que no es suficiente, pues al no contar con controles de seguridad y restricción y la claridad de su manejo, puede generar incidentes y fallos, que ocasionen pérdidas de los activos de la información.

Grafico 25: Conocimiento sobre procedimiento documentado para apagar los equipos

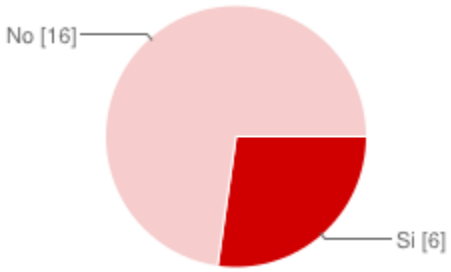


Respuesta	Encuestados	Porcentaje
Si	**0**	0%
No	**22**	100%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Grafico 26: Conocimiento sobre procedimiento documentado sobre manejo de la información

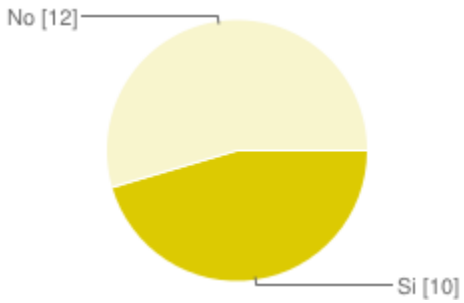


Respuesta	Encuestados	Porcentaje
Si	**6**	27%
No	**16**	73%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Grafico 27: Conocimiento sobre manejo de copias de respaldo



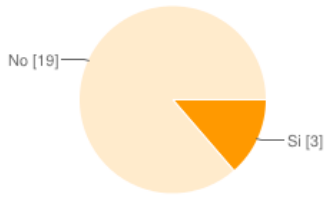
Respuesta	Encuestados	Porcentaje
Si	**10**	45%
No	**12**	55%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Continuando, con lo que respecta a procedimientos documentados y el conocimiento de los miembros de la organización sobre estos se observa; que un 100% de los miembros no conocen algo al respecto de apagar los computadores, el 27% conoce sobre procedimientos alrededor de seguridad de la información y solo el 45% sobre las copias de respaldo, esto demuestra, el bajo manejo sobre la seguridad de la información sus procedimientos y procesos, esto debido a la falta de comunicación sobre los mismos, la no capacitación y el no establecimiento de un SGSI que permita ser preventivos ante incidentes de seguridad de la información.

Grafico 28: Conocimiento sobre la eliminación segura de la información



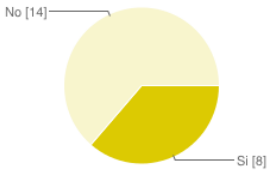
Respuesta	Encuestados	Porcentaje
Si	**3**	14%
No	**19**	86%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

En lo que respecta al manejo de la eliminación segura de la información el 86% de los miembros de la organización conocen el procedimiento, lo que es un buen indicador en la prevención y control de la seguridad de la información, logrando satisfacer una de las necesidades de la norma, pero que requiere llegar al total de los miembros de la empresa.

Grafico 29: Posee información de la empresa guardados en dispositivos personales



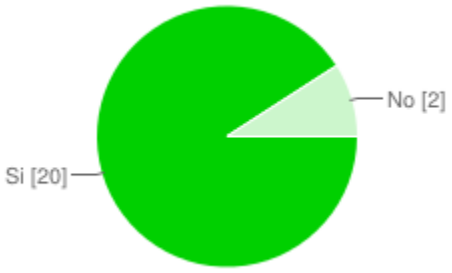
Respuesta	Encuestados	Porcentaje
Si	**8**	36%
No	**14**	64%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Aunque solo el 36% de los miembros de la organización tienen información de la empresa en sus dispositivos personales, este se constituye en un alto porcentaje, pues puede ocurrir un incidente de seguridad que ocasione pérdidas importantes para la empresa; de tal modo que esta es una situación que debe ser mejorada y trabajada.

Grafico 30: Computadores de la empresa manejan antivirus



Respuesta	Encuestados	Porcentaje
Si	**20**	91%
No	**2**	9%

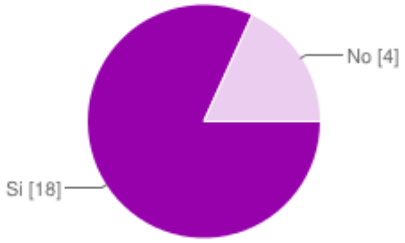
Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Un alto porcentaje de los computadores de la empresa manejan antivirus, sin embargo este es uno de los aspectos que debe ser logrado en su totalidad, teniendo en cuenta la importancia del antivirus para evitar eventos en la seguridad de la información.

La empresa posee un antivirus corporativo, pero que solo es conocido y manejado por el 91% y este no es vigilado en lo que respecta a la actualización y desinstalación; por ello, el inadecuado manejo puede ser causa de un incidente de seguridad.

Grafico 31: Restricción en el ingreso a la empresa de personal ajeno

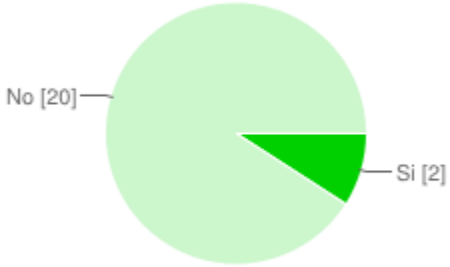


Respuesta	Encuestados	Porcentaje
Si	**18**	82%
No	**4**	18%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Grafico 32: Restricción del personal a páginas web



Respuesta	Encuestados	Porcentaje
Si	**2**	9%
No	**20**	91%

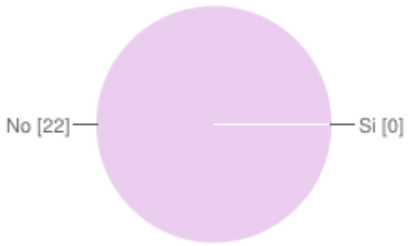
Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

En lo que respecta, a las restricciones es importante destacar que aunque la empresa tiene restricción al ingreso de personal externo a ella, solo el 82% del personal posee conocimiento de estos procedimientos y dispositivos asignados para ello, lo que significa que es importante capacitar sobre lo establecido con controles de acceso e ingreso a la planta e infraestructura física.

De la misma manera, continuando con las restricciones, los encuestados en el 91% manifiestan no tener información sobre el no ingreso a ciertas páginas web, lo que sugiere que el acceso es ilimitado, situación que puede ocasionar un incidente, a pesar de los antivirus que poseen los computadores.

Grafico 33: Capacitación sobre prevención de ataques informáticos o virus

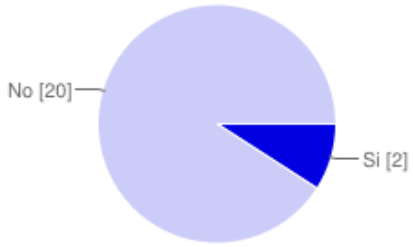


Respuesta	Encuestados	Porcentaje
Si	**0**	0%
No	**22**	100%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Grafico 34: Capacitación sobre manejo adecuado de usuarios y contraseñas



Respuesta	Encuestados	Porcentaje
Si	**2**	9%
No	**20**	91%

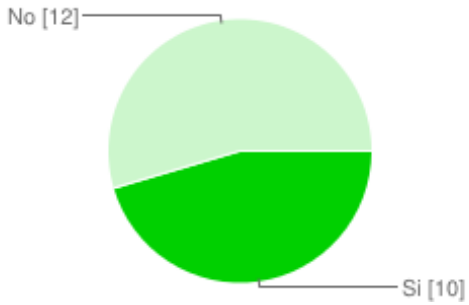
Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

La capacitación como elemento fundamental en la prevención de incidentes y desarrollo del Sistema de Gestión de Seguridad de la Información, la empresa se encuentra en un muy bajo nivel, ya que el 100% de los encuestados señala que no ha recibido capacitación para la prevención de ataques informáticos y el 91% de ellos señala lo mismo sobre el uso de usuarios y contraseñas, situación que debe observarse con detenimiento debido a la importancia de la capacitación en estos y otros aspectos en la prevención de situaciones anómalas en lo que respecta a la información y su seguridad.

En lo referente a la política de seguridad de la información, se señala como importante lo siguiente:

Grafico 35: Conocimiento sobre la existencia de una política de seguridad de la información



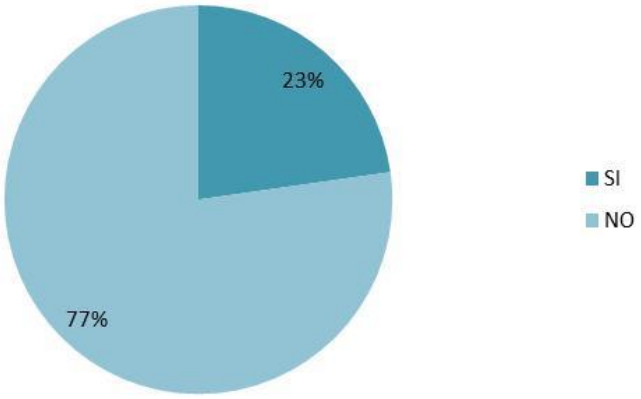
Respuesta	Encuestados	Porcentaje
Si	**10**	45%
No	**12**	55%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

El 55% de los miembros de la organización asegura no conocer una política de seguridad de la información, mientras el 45% dice conocerla, lo que permite observar que existe una ambigüedad al respecto, pues en realidad para cumplimiento de exigencias propias de unos clientes se crearon políticas adaptadas a las necesidades coyunturales, pero que no responden a la norma y que para nada constituyen la política de seguridad de la información de la empresa, de tal forma, que no hay un conocimiento y situación clara en lo que se refiere a la política de seguridad de la información.

Grafico 36: Conocimiento sobre la política de seguridad de la información



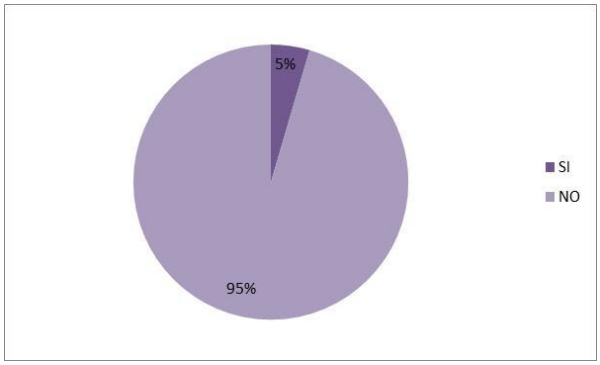
Respuesta	Encuestados	Porcentaje
Si	**5**	23%
No	**17**	77%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

De lo anterior, se concluye que al no existir una política de seguridad de la información clara y precisa, no existe socialización y conductos claros de lineamientos, procesos, controles y procedimientos de la misma.

Grafico 37: Socialización constante de la política de seguridad a los miembros de la empresa



Respuesta	Encuestados	Porcentaje
Si	**1**	5%
No	**21**	95%

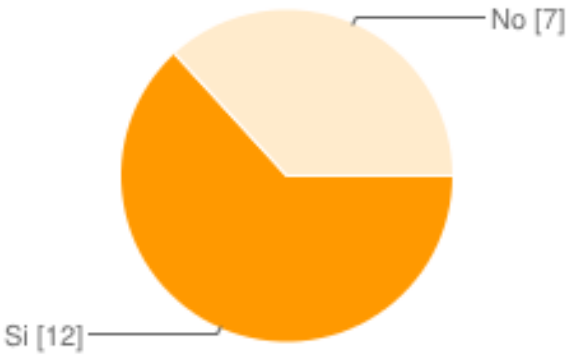
Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

Sin embargo, la mayoría de los encuestados el 54%, reconocen al (los) responsable (s) de la política de seguridad de la información, pero en realidad no existe alguien que cumpla este rol, lo que sucede es una asociación del jefe de ingeniería con el del responsable de seguridad de la información.

Ya que como se señaló anteriormente no existe en la empresa un oficial y/o comité de la seguridad; por tanto, no existe un responsable directo que lidere procesos y genere la política de seguridad de la información. La respuesta a la pregunta anterior es resultado de la mala información y los imaginarios de los miembros de la organización.

Grafico 38: Conocimiento del (los) encargado (s) de la política seguridad de la información



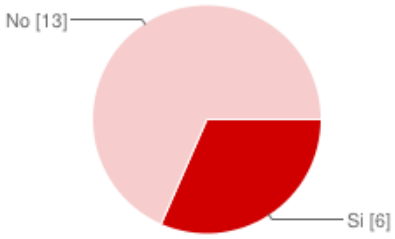
Respuesta	Encuestados	Porcentaje
Si	**12**	54%
No	**7**	32%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

El número de encuestados de la gráfica anterior no corresponde al total de los 22 miembros de la empresa, ya que 3 encuestados no responden o no saben sobre la pregunta anterior.

Grafico 39: Conocimiento sobre la capacitación de los responsables de la seguridad de la información



Respuesta	Encuestados	Porcentaje
Si	**6**	27%
No	**13**	59%

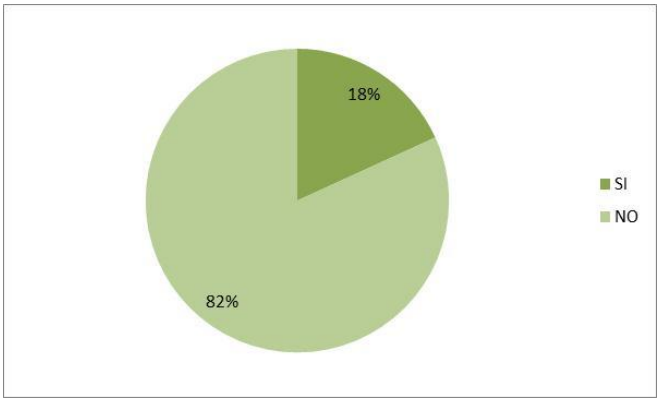
Fuente: Autor

Referencia: Encuesta Seguridad de la Información (julio de 2013)

El número de encuestados de la gráfica anterior no corresponde al total de los 22 miembros de la empresa, ya que 3 encuestados no responden o no saben sobre la pregunta anterior.

Igualmente, los miembros de la empresa no conocen mucho sobre el tema de seguridad de la información, pues no han recibido un plan de capacitación, ni siquiera al ingresar a la organización; y el 82% señala no conocer el plan de contingencia del sistema de seguridad de la información; toda vez que no existe un Sistema de Seguridad de la Información implementado y por lo tanto, los que dicen conocerlo es porque hacen parte del área de ingeniería y que por requerimientos de clientes externos han organizado algunos aspectos en ese orden y por tal motivo señalan planes y programas de capacitación, pero dichos planes, procedimientos y políticas no se han organizado debidamente.

Grafico 40: Conocimiento sobre el plan de contingencia del sistema seguridad de la información



Respuesta	Encuestados	Porcentaje
Si	4	18%
No	18	82%

Fuente: Autor

Referencia: Encuesta Seguridad de la Información (Agosto de 2013)

Por otro lado, es importante destacar que en lo referente al diagnóstico de la empresa con respecto a la seguridad de la información se observa significativamente lo siguiente:

En cuanto a las *condiciones físicas y la infraestructura* se evidencia, que la empresa aunque es pequeña no posee claridad en la seguridad y vigilancia de los recursos propios; al igual que no conserva la vigilancia adecuada y defensa de sus bienes e inmuebles, permitiendo el acceso a terceros de forma fácil y sin restricciones; igualmente no hay claridad en la manera de realizar protección y prevención de incendios.

Cuenta con las condiciones eléctricas y de protección de los procesadores y de la red inalámbrica en general, permitiendo proteger datos e información. Por ello, puede considerarse que la organización procura mantener las condiciones físicas y de infraestructura que permitan seguridad en la información.

En este mismo diagnóstico, en lo relativo a *seguridad de la información* propiamente dicha; la empresa tiene un bajo nivel de organización y gestión al respecto, pues no cuenta con políticas claras, responsables o procedimientos documentados; solo se puede destacar como elemento positivo lo que tiene que ver con las claves de acceso a los correos electrónicos y usuarios. La empresa debe asumir la importancia de los procesos en este tema y establecer los elementos pertinentes para dar cuenta de un Sistema Gestión Seguridad de la Información.

En lo referente a *recursos humanos*, la empresa no cuenta con procesos de sensibilización, inducción y capacitación permanente al personal sobre seguridad de la información, tampoco con responsables que lideren y concienticen a los miembros de la organización; de la misma forma no realiza las respectivas cláusulas de confidencialidad y demás necesarias en la protección de datos e información –a pesar de haber contado con un incidente al respecto-. Por todo ello, es necesario reforzar, sensibilizar y capacitar adecuadamente al personal.

Con respecto a las *comunicaciones*, a pesar de tener antivirus y cortafuegos institucionales, la empresa no restringe el acceso a las páginas en internet, situación que genera incidentes en la información; igualmente, no hay auditorias ni manejo de las copias de seguridad y demás, lo que propicia situaciones de riesgo en la información.

De esta manera después de analizados los resultados de la encuesta se puede concluir:

1. No existe claridad sobre procesos y procedimientos de seguridad de la información por parte de la gran mayoría de los miembros de la empresa

2. Los miembros que conocen aspectos relacionados con la seguridad, la política y el sistema son parte del área de ingeniería, que en últimas son los responsables de dichos procesos.
3. No existe una capacitación e información clara al ingreso a la empresa en la que se defina todo lo referente al manejo y uso de la información, situación que puede generar incidentes graves.
4. No existen procedimientos documentados que permitan prevenir incidentes en el manejo de la información y no existe el conocimiento de los mismos por parte de los miembros de la empresa
5. No se conoce jornadas y capacitaciones a los miembros de la empresa sobre los controles y el manejo de la seguridad de la información.
6. No existe una cultura de la seguridad de la información, generando compromisos y sensibilizando sobre el cuidado y protección de la información.

En este sentido, es necesario implementar una metodología que permita a través de un proceso claro y pertinente, la creación de una política de seguridad de la información, que dé cuenta de las necesidades particulares de la empresa.

Así, la metodología de generación de política de seguridad de la información, diseñada por el grupo Nyquist de la Universidad Tecnológica de Pereira, permitirá a través un ejercicio metódico, ir construyendo los lineamientos, procedimientos y controles que genere la política de seguridad y a largo plazo un SGSI

Después de estudiada por la Alta Dirección, la metodología, se aprueba su implementación para la consolidación de una política de seguridad de la información para la empresa., proceso que se da después del diagnóstico y la evaluación de los activos de la información anteriormente presentados.

Se recomienda construir una política que se adapte a la necesidades y requerimientos de la empresa; toda vez, que la organización es pequeña en recursos humanos, tiene clientes de un alto nivel y se potencializa en su mercado como una de las de mayor crecimiento.

7.2. IMPLEMENTACIÓN DE LA METODOLOGÍA DE GENERACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA. BOGOTÁ D.C.

7.2.1. Planear

En este primer aspecto, se designarán los insumos necesarios para la implementación de la metodología para la generación de la política de la seguridad de la información en la empresa. ubicada en la ciudad de Bogotá; que entre otros contarán con objetivos, procesos y procedimientos, que estarán actuando de acuerdo a las necesidades propias de la empresa y los requerimientos de la misma.

7.2.2. Nombrar el líder del proyecto y el oficial de seguridad de la información.

La alta dirección de la empresa, en reunión realizada el día miércoles 25 de septiembre y en decisión por unanimidad, resuelven designar como responsable del proceso de seguridad de la información al ingeniero electrónico Elier Mauricio Noguera (ver anexo 2), *director de desarrollo*, que cuenta con ocho (8) años en la empresa; en este sentido desde el momento asumirá el rol de sponsor y director del proyecto, por ser uno de los funcionarios con mayor experiencia en el campo, con el liderazgo y autoridad suficientes para llevar con éxito dicho proceso[24].

[24] Aunque la metodología de generación de política de seguridad de la información creada por el grupo Nyquist, sugiere un sponsor y director independiente, la empresa., por contar con un número reducido de miembros, considera asignar el cargo de sponsor y director del proyecto al ingeniero Elier Mauricio Noguera, que cuenta con la experiencia, idoneidad y autoridad necesaria para la toma de decisiones en el desarrollo del proyecto.

7.2.3. Nombrar el oficial de Seguridad de la Información

De la misma, la alta dirección en encuentro realizado el día miércoles 25 de septiembre, deciden nombrar a un estudiante en proceso de grado de ingeniería de sistemas y computación; como oficial y líder de seguridad, ya que cuenta con la experiencia, el saber necesario para ejecutar dicha labor y posee conocimientos claros y precisos sobre la norma ISO 27000 y 27001[25].

El oficial de la seguridad de la información de la empresa., cuenta con el liderazgo necesario dentro de la empresa y cuenta con el tiempo y la dedicación necesarios para llevar con éxito la tarea asignada[26].

7.2.4. Propuesta del proyecto de generación de la política y procedimientos de seguridad de la información.

7.2.4.1. Definir objetivos y alcances del proyecto

Teniendo en cuenta las necesidades de la empresa., en lo relativo a la seguridad de la información y contando con los requerimientos y exigencias normativas y legales, se propone a continuación algunos elementos indispensables para la elaboración del proyecto que permitirá la generación de la política de seguridad de la información:

La política de seguridad de la información en la empresa, debe incluir la posición de la empresa en lo referente a la seguridad de los activos de la información, el cargo y nombre del responsable del proceso, quien mantendrá informado

[25] De la misma forma, aunque la recomendación del grupo de investigación Nyquist, es la de contar con un líder y oficial de seguridad independiente, las limitaciones de recursos humanos, conlleva a que la Alta Dirección designe al ingeniero Guillermo Rodríguez Gahona, como responsable en estas dos tareas, ya que desarrolla su trabajo de grado en la ejecución de la metodología.

[26] El oficial de seguridad de la información de la empresa. cumple con los requerimientos ofrecidos en la metodología de generación de política de seguridad de la información, diseñada por el grupo de investigación Nyquist de la Universidad Tecnológica de Pereira. P. 6 -7.

constantemente a la alta dirección y todos los miembros de la empresa de la aplicabilidad de la política.

De igual manera la política de seguridad de la información de la empresa., estará dirigida a todas las áreas y miembros de la empresa e igualmente a los clientes y proveedores de la misma, teniendo en cuenta las particularidades y exigencias de los clientes y estrategias de los vendedores

Es importante que la política de la seguridad de la información de la empresa., determine claramente las excepciones y el procedimiento a seguir en caso que se produzcan.

Otros aspectos a tener en cuenta para la generación de la política de seguridad de la información de la empresa., es el tiempo de vigencia de la misma y el procedimiento para su obsolescencia.

Es necesario denotar, que la empresa requiere de un sistema de seguridad de la información, debido a la expansión que experimenta en los últimos años, la exigencia de los clientes recientes lleva a la organización a contar con la protección y seguridad debida de la información; por todo ello se plantea una metodología de generación de política de seguridad, que cumpla con las expectativas y necesidades organizacionales para atender necesidades de los clientes y regular los procesos y procedimientos relacionados con los activos de información.

En este sentido, los objetivos y alcance del proyecto, para la creación de la política de seguridad de la información en la empresa, son los siguientes:

7.2.4.2. Objetivo general

Resguardar los recursos y activos de la información de la empresa. por parte de los miembros de la organización y terceros que actúan como clientes y proveedores; a través de la ordenación de procesos y procedimientos documentados, que permitan establecer seguimientos y acciones correctivas frente a las posibles fallas o incidentes de seguridad.

7.2.4.3. Objetivos específicos

Formalizar los recursos humanos, físicos y presupuestales necesarios para la implementación de la política de seguridad de la información.

Comunicar a los miembros de la organización la política de seguridad de la información, capacitando sobre ella en relativos periodos de tiempo.

Generar una cultura de seguridad de la información, permitiendo que los miembros de la organización tomen conciencia de la importancia de proteger y resguardar la información.

Establecer los procedimientos, estándares, mejores prácticas y la guía que soporte la política de seguridad de la información.

7.2.4.4. Alcance

La política de seguridad de la información, se aplica a toda la empresa y cada una de sus dependencias, áreas y direcciones e igualmente a los activos y recursos que hacen parte de la organización. Para los que actúen como terceros -clientes y proveedores u otros- La política de seguridad de la información dependerá de las excepciones y condiciones que determiné el comité de seguridad.

De este modo la organización la empresa., dispone en la política de seguridad de la información, los siguientes aspectos en relación al alcance de la misma:

1. Clasificación y vigilancia de activos:
2. Seguridad física y medio ambiental:
3. Gestión de las comunicaciones y operaciones
4. Seguridad del personal
5. Control de acceso

7.2.4.5. Requerimientos del recurso humano del proyecto

Para la implementación de la política de seguridad de la información, de la empresa., se contará con el siguiente recurso humano, funciones, perfiles y características:

1. Sponsor y gerente del proyecto: el patrocinador del proyecto, quién gestionará los recursos para la realización de este y velará por el cumplimiento de las metas será un ingeniero, miembro de la organización que cuenta con los años de experiencia y autonomía necesaria para dar cumplimiento a los objetivos del proyecto.

Tiempo de permanencia en la empresa: ocho (8) años

Perfil: Ingeniero de Sistemas, Ingeniero Electrónico o Ingeniero de Telecomunicaciones
Postgrado en áreas de Teleinformática
Manejo en Microsoft Visual Studio / .Net (Preferiblemente C++ y/o C#)
Integración de Aplicaciones con Bases de datos
Mínimo 2 cursos certificados de Microsoft
Sistema de Gestión de Calidad ISO 9001:2000
2 años de experiencia en Visual Studio/.NET
2 años de experiencia en Computer Telephony y/o desarrollo de software en Teleinformática

3 años ejerciendo su profesión

Funciones dentro de la empresa:

a. Liderar el proceso de adopción y uso de una metodología de desarrollo que permita:
- Controlar y tercerizar el desarrollo.
- Reducir costos en el proceso.

b. Asegurar la calidad del desarrollo.
c. Implementar desarrollos documentados, eficientes y organizados.
d. Usar nuevas tecnologías en la implementación.
e. Liderar el desarrollo de componentes críticos y/o especializados (interfaces gráficas, bases de datos, componentes, SDK de integración, etc) que permitan cumplir con los requerimientos planteados en el diseño de las soluciones.
f. Ejecutar desarrollos y pruebas internas o tercerizadas.
g. Garantizar que los desarrollos cumplan con altos componentes tecnológicos de acorde a las políticas de calidad de la compañía.
h. Plantear mejoras y nuevas características a las soluciones existentes.

Funciones dentro del proyecto:

a. Gestionar los recursos humanos, físicos y presupuestales para la ejecución del proyecto
b. Revisar los avances y procedimientos realizados en la generación de la política de seguridad de la información de la empresa
c. Mantener comunicación permanente con el líder y oficial de seguridad en los avances y desarrollo del proyecto.
d. Mantener informada a la Alta Dirección sobre el desarrollo y avance del proyecto de generación de la política de seguridad de la información.

2. Líder y oficial de seguridad del proyecto: se designa al ingeniero en diseños de aplicaciones Guillermo rodríguez Gahona, quién asumirá la responsabilidad de direccionar el proyecto hasta el cumplimiento de los objetivos.

Tiempo de permanencia en la empresa: dos (2) años

Perfil:

1 año de experiencia en proyectos de análisis y diseño de sistemas de información orientado a objetos
1 año de experiencia demostrable en uso de herramientas colaborativas y de comunicación.
1 año de experiencia en el desarrollo sobre Visual Studio / .Net (preferiblemente C# y/o ASP. NET)

Funciones dentro de la empresa:

a. Responsable de la elaboración, corrección y mejora de los manuales y la documentación según la política de calidad de la compañía.
b. Participar activamente en el análisis y diseño de las nuevas soluciones, utilizando el proceso establecido por la compañía y el lenguaje UML.
c. Responsable del mantenimiento, operación y aseguramiento del código fuente y la documentación.
d. Responsable de mantener actualizada la documentación, código fuente y cronogramas, así como la publicación en la página web de la información relacionada con el área de Ingeniería.
e. Efectuar Control de Calidad y pruebas de los productos desarrollados.
f. Elaborar la documentación de Técnica de las Soluciones.

Funciones dentro del proyecto:

a. Crear propuesta del proyecto de generación de la política y procedimientos de seguridad de la información.

b. Gestionar la inscripción y autorización del proyecto al interior de la organización.
c. Gestionar los recursos humanos y presupuestales para el desarrollo del proyecto.
d. Designar los grupos de trabajo de seguridad de la Información.
e. Definir los roles y responsabilidades del comité de seguridad y sus subgrupos de trabajo
f. Revisar la propuesta del proyecto para generar la política y procedimiento de seguridad de la información.
g. Ajustar la propuesta del proyecto para generar la política y los procedimientos de seguridad de la información.
h. Gestionar la aprobación del proyecto de generación de la política y procedimientos de seguridad de la información.
i. Formar y capacitar en seguridad de la información, metodología de generación de la política y procedimientos de seguridad de la información.
j. Recolectar los insumos necesarios para la creación de la política y procedimientos de seguridad de la información.
k. Realizar los ajustes finales a la política de seguridad de la información.
l. Socializar la política de seguridad de la información a cada uno de los integrantes, dependencias y áreas de la empresa.
m. Definir y desarrollar los procedimientos de seguridad de la información.
n. Definir los procedimientos para solicitar excepciones de aplicación de la política
o. Establecer los roles y responsabilidades de los procedimientos de seguridad de la información.
p. Definir las estrategias de socialización y sensibilización de todo el personal frente a la política y procedimientos de seguridad de la información.
q. Proponer el cronograma para la socialización y las jornadas de sensibilización de la política y los procedimientos de la seguridad de la información.

r. Ejecutar el cronograma de socialización y sensibilización del personal de la política y procedimientos de seguridad de la información.
s. Realizar entrega oficial de la política, sus lineamientos y procedimientos totalmente terminados y socializados a los grupos de interés y a la Alta Dirección para su implementación.[27]

3. Comité de seguridad: se encuentra integrado por un representante de cada una de las áreas que componen la organización:

Cargo: Director administrativo y financiero
Perfil: Profesional en administración de empresas
Tiempo en la empresa: Febrero de 2010

Cargo: Asistente administrativo y financiero
Perfil: Bachiller académico
Tiempo en la empresa: Mayo de 2013

Cargo: Ingeniero de soporte
Perfil: Técnico en sistemas
Tiempo en la empresa: Enero 2006

Cargo: Director de desarrollo
Perfil: Ingeniero electrónico
Tiempo en la empresa: Enero de 2005

Cargo: Ingeniero de diseño de aplicaciones
Perfil: Proceso de grado ingeniería de sistemas y computación
Tiempo en la empresa: 2 años

[27] Metodología de generación de política de seguridad de la información. Grupo de investigación Nyquist, julio 30 de 2013. Pereira, Risaralda

El comité de seguridad de la información tendrá entre otras funciones las siguientes:

a. Asegurar que las metas de la seguridad de la información están inidentificadas, satisfacen los requisitos de la organización y que se encuentren integradas a los procesos pertinentes.
b. Formular, revisar y aprobar la política de seguridad de la información.
c. Revisar la eficacia de la implementación de la política de seguridad de la información.
d. Proporcionar los recursos necesarios para la seguridad de la información.
e. Aprobar la asignación de funciones y responsabilidades específicas para la SI en toda la organización.
f. Asegurar la coordinación en toda la organización de la implementación de los controles de seguridad de la información.
g. Identificar las necesidades de asesorías internas o externas sobre seguridad de la información y revisar sus resultados.
h. Dependiendo del tamaño de la organización, tales responsabilidades se podrían manejar a través de un comité de dirección dedicado a esta labor o a través de un organismo de dirección ya existente, como por ejemplo el consejo directivo.

4. Un representante de cada una de las áreas[28]

Cargo: Director administrativo y financiero
Área. Administrativa

Cargo: Director de desarrollo
Área: Ingeniería

[28] La metodología desarrollada por el grupo de investigación Nyquist, señala dos representantes por cada una de las áreas de la empresa; sin embargo la empresa. por ser una empresa de tan solo 20 funcionarios, designa un solo representante, que a su vez harán parte del comité de seguridad de la información.

Cargo: Sales and Marketing Director
Área: comercial

Cada uno de los anteriores funcionares serán parte de la organización –no se trabajará con agentes externos que cumplan estas funciones-.

Necesidades del personal:

a. Recursos físicos y presupuestales acordes a las necesidades del proyecto (pc, papelería, teléfonos, etc.)
b. Espacios y tiempos designados para la ejecución del proyecto (reuniones, elaboración de documentos, etc.)

Habilidades del personal:

a. Capacidad de liderazgo y proactividad
b. Cumplimiento de objetivos
c. Capacidad de gestión y resolución de problemas
d. Manejo de público
e. Conocimientos básicos en gestión de seguridad de la información
f. Trabajo en equipo
g. Capacidad para desplegar acciones
h. Mayor capacidad analítica

7.2.4.6. Presupuesto del proyecto

Para la ejecución y desarrollo del proyecto se hace necesario contar con los siguientes recursos:

Tabla 1: Presupuesto global

	FUENTE	TIEMPO	VALOR TOTAL
Recurso Humano	la empresa	160 Horas	3200000
Equipos	la empresa	160 Horas	480000
Material	la empresa	NA	20000
Derechos Y Propiedad Intelectual	la empresa	NA	NA
Jornadas de capacitación, socialización y sensibilización	la empresa	160 Horas	3200000
Jornada de reuniones (Alta gerencia, Comité de seguridad de la información)	la empresa	24 Horas	960000

Los tiempos están dados en horas, y son tomados de forma lineal.

Los valores totales están dados en pesos colombianos

7.2.4.7. Cronograma del proyecto

Tabla 2: El siguiente es el cronograma con el que se pretende ejecutar el proyecto.

ACTIVIDADES	OCT	NOV	DIC	ENE	FEB
PLANEAR					
Asignación de sponsor y director del proyecto					
Designación del líder y oficial de seguridad					

Creación la propuesta del proyecto de generación de la política y procedimientos de seguridad de la información					
Inscripción y autorización del proyecto al interior de la organización					
Gestión recursos humanos, físicos y presupuestales para la ejecución del proyecto					
Definición le personal que participará en el proyecto					
Revisión de la propuesta del proyecto					
Ajustes de la propuesta del proyecto					
Gestión de la aprobación definitiva del proyecto					
Capacitación del personal en seguridad de la información, en la política y sus respectivos procedimientos					
Realización de los inventarios de activos de la información					
Realización de matriz de riesgo de información					
Asignación de normatividad aplicable					
Definición del alcance del sistema seguridad de la información					
Elaboración de documentos previas de la política de seguridad de la información					
Informe de auditoria					
Elaboración de formato para la política y lineamientos de seguridad de la información					
HACER					
Análisis de los insumos por parte del comité de seguridad					
Formulación la política general y sus lineamientos para cada uno de los controles o procesos					

Creación de la política general					
Creación de los lineamientos basados en las clausulas y controles					
Ajuste de la política y lineamientos generados al interior del subgrupo de trabajo					
Presentar el primer borrador de la política en las áreas de trabajo					
Realizar los ajustes al primer borrador de la política					
Presentar el segundo borrador de la política en las áreas de trabajo					
Ajustes al borrador de la política por parte del comité de seguridad de la información					
Socialización de las política, sus procedimientos a las directivas, dependencias y áreas					
Modificación del documento de la política ante las sugerencias de los miembros de la organización					
Aprobación del documento de la política de seguridad de la información por parte de la Alta Dirección					
Definición de los procedimientos de seguridad de la información					
Propuesta de implementación de procedimientos para cada uno de los lineamientos de la política de seguridad					
Identificación de los riesgos asociados a los procedimientos de implementación de la política con sus respectivos controles					
Definición de procedimientos para solicitud de excepciones de la política					
Establecimiento de roles y responsabilidades de los procedimientos					
Aprobación de los procedimientos de seguridad de la información					
Definición de las estrategias de socialización y sensibilización de la política seguridad de la información					

Publicación de la política, estándares y procedimientos aprobados					
Entrega oficial de la política, sus lineamientos y procedimientos totalmente terminados y socializados					

1. En primera instancia la política de seguridad de la información de la empresa debe permitir una adecuada y eficiente ***clasificación y vigilancia de activos***, que reconozca la protección de los mismos, evitando incidente y situaciones de criticidad.
2. Por otro lado, el alcance de la política tendrá como elemento fundamental determinar la seguridad de la información en lo relacionado a los ***recursos humanos, físicos e incidentes medio ambientales,*** representando los problemas más importantes en lo que respecta a los riesgos de la seguridad; por ello la política determina su alcance a la prevención, capacitación y organización de dichos recursos y situaciones endógenas y exógenas.

7.3. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DE LA EMPRESA.

7.3.1. Introducción

La empresa., entiende la importancia de proteger y salvaguardar la información, como activo que representa elemento fundamental para el logro de los objetivos y el desarrollo de la misión; en este sentido, la empresa busca generar un Sistema de Gestión de Seguridad de la Información que establezca los criterios necesarios para hacer del manejo de ella un ejercicio eficiente y eficaz.

Nuestra empresa tiene riesgos y amenaza a la información, que deben ser detectados para lograr la prevención y evitar dificultades internas y externas; razón por la cual, se ha generado una política de seguridad de la información que

propone los requerimientos y lineamientos necesarios para que los usuarios internos como externos, hagan un uso adecuado de los activos de información de nuestra organización.

7.3.2. Definiciones y criterios de seguridad y calidad

La empresa define una política de seguridad de la información, para generar buenas prácticas y una cultura de eficiencia y eficacia en el manejo de la información, que permita satisfacer necesidades de los clientes y garantizar el logro de los objetivos organizacionales.

Por ello, la política de nuestra organización se sustenta en las normas, leyes y lineamientos macros establecidos para la seguridad de la información en el país.

la empresa Atiende entre otras normas la 052 de la Superintendencia Financiera de Colombia, la cual establece las siguientes definiciones de seguridad que deben cumplir los sistemas del cliente:

Para el cumplimiento de los requerimientos mínimos de seguridad y calidad de la información que se maneja a través de canales y medios de distribución de productos y servicios para clientes y usuarios, las entidades deberán tener en cuenta las siguientes definiciones y criterios:

7.3.3. Criterios de Seguridad de la información:

a) Confidencialidad: Hace referencia a la protección de información cuya divulgación no está autorizada.

b) Integridad: La información debe ser precisa, coherente y completa desde su creación hasta su destrucción.

c) Disponibilidad: La información debe estar en el momento y en el formato que se requiera ahora y en el futuro, al igual que los recursos necesarios para su uso.

7.3.4. Criterios de Calidad de la información

a) Efectividad: La información relevante debe ser pertinente y su entrega oportuna, correcta y consistente.

b) Eficiencia: El procesamiento y suministro de información debe hacerse utilizando de la mejor manera posible los recursos.

c) Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones."[29]

Igualmente, para la consolidación de la política de seguridad de la información, la empresa se soporta de la norma ISO 9000, 9001, 27000 y 270001, que se han constituido en pilares constitutivos de la cultura organizacional de la empresa.

7.3.5. Objetivos

7.3.5.1. Objetivo General

Resguardar los recursos y activos de la información de la empresa. por parte de los miembros de la organización y terceros que actúan como clientes y proveedores; a través de la ordenación de procesos y procedimientos documentados, que permitan establecer seguimientos y acciones correctivas frente a las posibles fallas o incidentes de seguridad.

[29] Superintendencia Financiera de Colombia, 2007, P. 97

7.3.5.2. Objetivos específicos

Comunicar a los miembros de la organización la política de seguridad de la información, capacitando sobre ella en relativos periodos de tiempo.

Generar una cultura de seguridad de la información, permitiendo que los miembros de la organización tomen conciencia de la importancia de proteger y resguardar la información.

Mantener actualizada la política de seguridad de la información, frente a los posibles cambios o necesidades que con el paso del tiempo se van gestando al interior de la organización.

7.3.6. Alcance

La política de seguridad de la información, se aplica a toda la empresa y cada una de sus dependencias, áreas y direcciones e igualmente a los activos y recursos que hacen parte de la organización. Para los que actúen como terceros -clientes y proveedores u otros- La política de seguridad de la información dependerá de las excepciones y condiciones que determiné el comité de seguridad.

De este modo la organización la empresa., dispone en la política de seguridad de la información, los siguientes aspectos en relación al alcance de la misma:

6. Clasificación y vigilancia de activos:
7. Seguridad física y medio ambiental:
8. Gestión de las comunicaciones y operaciones
9. Seguridad del personal
10. Control de acceso

7.3.7. Recursos humanos

Para la ejecución y desarrollo de la política de seguridad de la información, la organización cuenta con los siguientes recursos humanos, que permiten las buenas prácticas, regulan los controles y procedimientos en el perfeccionamiento de la política:

a. Alta Dirección: encargada de realizar la revisión final de la política y aprobarla para su ejecución.

b. **Gerente del proyecto:** el App Dev Manager de la empresa es el gerente y sponsor en el establecimiento y desarrollo de la política de seguridad de la información.

c. **Líder y oficial del proyecto de seguridad de la información:** el ingeniero de diseño de aplicaciones, es el encargado de liderar y organizar todo lo relacionado con la política de seguridad de la información

d. **Comité de seguridad de la información:** debido a que la empresa se encuentra constituida por un número de miembros limitado, el comité se organiza contando con un miembro de cada una de las áreas que constituyen la organización. (Un representante del área administrativa, un representante del área comercial, un representante del área de ingeniería y el oficial de seguridad de la información).

e. **Dueños de los procesos:** son parte indispensables de los recursos humanos en la ejecución y desarrollo de la política de seguridad de la información. Entre los procesos se encuentran.

Proceso administrativo: proceso de recursos humanos y proceso de contabilidad

Proceso de ingeniería: proceso soportes, proceso desarrollo y proceso diseño de aplicaciones

Proceso comercial: proceso comercial y proceso ventas.

7.3.7.1. Responsabilidades internas y externas

La política de seguridad de la información de nuestra organización, será responsabilidad de todos y cada uno de los miembros que constituyen la empresa, sin excepción alguna y atendiendo a las directrices y parámetros exigidos por el comité y oficial de seguridad de la información.

En lo que respecta a los externos su responsabilidad depende de las acciones particulares establecidas por el comité de seguridad de la información, tanto para los proveedores como para los clientes.

Responsabilidad de la Alta Dirección: es la responsable de revisar y aprobar la política de seguridad de la información, aprobar sus cambios y destinar el presupuesto necesario para el SGSI

Responsabilidad del oficial de seguridad de la información: liderar la implementación de una cultura de seguridad de la información, generar canales de comunicación para la socialización de la política y acompañar al comité de seguridad de la información en la formulación de la política, lineamientos, controles y procedimientos.

Responsabilidad del comité de seguridad de la información: formular, revisar la política de seguridad de la información, realizar los lineamientos, procedimientos y controles necesarios para ejecutar la política.

Implementar la política en todos sus niveles y directrices, gestionar los recursos necesarios para dicha implementación.

Responsabilidad dueños de los procesos: determinar la información sensible, custodiarla e informar al oficial y comité de seguridad de la información, sobre las posibles amenazas de la información sensible de la empresa.

Responsabilidad de los miembros de la organización: todos y cada uno de los miembros de la empresa., es responsable de la información en custodia de su

cargo, a la que accedan y requieran, reportando cualquier falla o incidente que se presente.

7.3.7.2. Comité de seguridad de la información

El comité de seguridad de la empresa., es el encargado de controlar, formular y socializar la política de seguridad de la información y entre sus funciones se encuentra:

- Revisar la eficacia de la implementación de la política de seguridad de la información.
- Proporcionar los recursos necesarios para la seguridad de la información
- Velar por el cumplimiento de las políticas, lineamientos, procedimientos y demás documentos relacionados con la seguridad de la Información dentro de la organización.

Y se encuentra conformado por un representante de cada una de las áreas de la empresa (área administrativa, comercial, ingeniería) y por el oficial de seguridad de la información.

7.3.8. Políticas generales

La empresa ha establecido las siguientes políticas generales de la seguridad de la información

a. La seguridad de la Información se considera como prioritaria en la cultura organizacional de la empresa.
b. la empresa contará con una clasificación rigurosa de sus activos, según lo específica la norma ISO 27001, realizando actualización de la misma periódicamente.

c. El comité de seguridad de la información en la empresa. será el encargado de velar por el cumplimiento de la política y monitoreo de los controles de la misma.
d. Los controles implementados por la empresa. para desarrollar y cumplir la política seguridad de la información, serán verificados constantemente y replanteados si llegado el caso no tuvieran la eficacia requerida.
e. Todos los funcionarios serán responsable de la información a la que accedan y deberán protegerla de cualquier pérdida, alteración y uso indebido.
f. la empresa solo hará uso de software adquiridos legalmente y que cuenten con los requisitos establecido por la ley.
g. la empresa realizará auditorias, supervisión y controles permanentes a cada uno de los procesos de la organización en lo referente a la seguridad de la información, para establecer acciones preventivas.
h. Cualquier violación a la seguridad de la Información, será reportado, monitoreado y se le realizará el seguimiento necesario.
i. La empresa desarrolla los lineamientos, procedimientos y controles necesarios para dar cumplimiento a la política seguridad de la información.
j. Igualmente la empresa. dispone de otras políticas, lineamentos, procedimientos y controles, que se refieren a continuación:

7.3.9. Activos de la información

La empresa, cuenta con diversos activos de la información, su clasificación se puede observar en el (anexo 4).

7.3.10. Clasificación de la información

Los activos de seguridad de la Información de la empresa, se encuentran clasificados en crítica (lista de precios, ventas, lista de canales, acuerdos de

confidencialidad, etc.), muy importante (órdenes de compra, etc), importante (lista de clientes, cotizaciones, factura, etc), poco importante (documentos de proyectos, indicadores, etc.) y baja (Brochures, publicidad, etc). Esta fue la clasificación inicial dada por los dueños de los procesos y ratificada por el comité de seguridad; sin embargo ante las actualizaciones, la normatividad vigente y los requerimientos de la política, dicha clasificación puede variar.

7.3.11. Propietarios de activos de la información: en la empresa.

Para la identificación de los propietarios de activos de la información, remitirse a la matriz de activos (anexo No. 4).

7.3.12. Uso de los activos de la información:

Los activos de la información serán de uso exclusivo de cada uno de los dueños de los procesos, quienes mantendrán vigente y regularán los controles para la protección de la información.

Los activos de la información serán clasificados y resguardados por cada dueño de proceso y en caso de presentarse anomalías o incidentes, realizarán oportunamente el reporte al oficial de seguridad y este inmediatamente al comité de seguridad, quienes en conjunto tomarán las acciones correctivas necesarias para solucionar dicho incidente.

Para el acceso al software teamsystem en el que reposa la gestión documental y de información de la empresa, será exclusivo para miembros de la organización, pero con restricción según perfil. Para ingresar a teamsystem, cada usuario se registra con usuario y contraseña contra el servidor de dominio de la empresa.

7.3.13. Requerimientos de contratos con terceros para el manejo de la información

Debido al tipo de información que maneja la empresa, esta tendrá permanente control sobre la información que se maneja con terceros; de tal forma que establecerá según el caso, acuerdos de confidencialidad, que beneficien tanto a la empresa, como a los clientes y proveedores; dicho acuerdos se establecerán en doble vía, debido a que muchos de los clientes de la empresa. poseen políticas específicas de seguridad de la información.

Los terceros deberán comprometerse a no divulgar, usar o explotar la información a la que tuvieren acceso de la empresa. y privilegiar la confidencialidad de dicha información.

7.3.14. Contratos y confidencialidad

Todos aquellos miembros de la organización, al ingresar a la empresa, deberán firmar un acuerdo de confidencialidad, que será parte integral del contrato laboral; dicho acuerdo de confidencialidad debe evidenciar por contratista los siguientes aspectos: el tipo de información a manejar, el uso de la información, los permisos para la salida de información y las consecuencias éticas y legales en caso de violación del contrato. Cuando se cambian de roles o existe un retiro de la empresa se notificará al oficial de seguridad de la información, para realizar el bloqueo del usuario o cualquier forma de acceso a la información de la información.

7.3.15. Capacitación de los usuarios

Todos los miembros de la organización, contarán al ingreso a la empresa de una capacitación y orientación de los lineamientos, controles y procedimientos de seguridad de la información.

Igualmente, en periodos relativos de tiempo se realizarán capacitaciones, por nuevos controles lineamientos o procedimientos que se generen desde la actualización de la política de seguridad de la información.

Los usuarios externos, sea por contrato como clientes o proveedores, recibirán capacitación sobre la política de seguridad de la información con los lineamientos básicos, que permitirá minimizar riesgos y establecer acuerdos.

7.3.16. Acceso a internet

La internet es fundamental para el trabajo diario de cada uno de los miembros de la empresa; por ello es fundamental el uso adecuado y correcto del mismo, ya que el mal uso puede suscitar riesgos y ataques a la información que se resguarda en los equipos de los miembros.

a. No se admite:

El ingreso a páginas que atenten contra la ética personal o de la empresa, que vaya en contradicción a los requerimientos legales nacionales, internacionales o políticas y lineamientos de la organización, tales como: pornografía de todo tipo, drogas, juegos en línea, etc.

El uso de redes sociales tipo Facebook, Skype, mensajería instantánea, yahoo, msn, y otros, para realizar actividades personales e intercambio de información que no sea autorizado por la empresa.

Descargar juegos, programas, protectores de pantalla, software, películas y música que no estén autorizados por los responsables y que atenten con la propiedad intelectual o el derecho de autor.

b. Cada uno de los miembros de la organización debe hacer un uso adecuado de los recursos de la organización, utilizándolo para uso exclusivo de sus funciones dentro de la empresa, cualquier irregularidad al respecto debe ser informada al oficial de seguridad de la información
c. Cualquier instalación o descarga de software que tengan una finalidad personal y no apliquen a la empresa, debe recibir la aprobación del oficial de seguridad y realizar el procedimiento establecido para tal caso.

7.3.16.1. Correo electrónico

Cada uno de los miembros de la empresa (a excepción de la persona de servicios generales) cuenta con un correo institucional que es asignado con la primera letra del nombre punto y el primer apellido completo, seguido de @nombre de la empresa y administrado por el App Dev Manager, cada usuario de correo electrónico debe contar con:

a. La clave del correo electrónico debe ser alfa numérica mayor a ocho caracteres y no contener en ella el número de la cédula, debe ser cambiada regularmente, para disminuir el riesgo en el plagio de la misma.
b. La cuenta de correo electrónico es de uso exclusivo para temas relacionados con las funciones del cargo y debe ser administradas con integridad, responsabilidad y honradez.
c. Los mensajes contenidos en la cuenta de correo son de propiedad de exclusiva de la empresa.
d. Los correos electrónicos no deben usarse para enviar o recibir ningún tipo de cadena, de tipo religioso, político sexista u otro similar, que generen

algún tipo de ataque o que atenten contra la integridad de la empresa y su ética.

e. Por ningún motivo se hará uso del correo electrónico para enviar o abrir extensiones ejecutables, para este tipo archivos se debe utilizar un ftp.
f. Toda información que haga parte de la empresa debe ser enviada exclusivamente por el correo electrónico institucional, no se admite el envío de información de la organización por el correo personal.
g. Los correos enviados deben incluir en la firma los logos corporativos, el cargo y responsable del envío y contar con las normas establecidas por la organización.

7.3.17. Instalación de software

Las aplicaciones son fundamentales para el buen desempeño y logro de los objetivos organizacionales y más si se sabe que la empresa., es una empresa prestadora de estos servicios; por tal motivo:

No se permite ningún tipo de instalación de software sin previa autorización del comité de seguridad y la alta dirección y si dicha instalación fuere aprobada por requerimientos exclusivos del logro de los objetivos organizacionales, será el proceso de soporte técnico quién instale y reglamente lo necesario para el nuevo software, estableciendo procedimiento de uso y acceso.

El personal de soporte técnico debe realizar mensualmente los inventarios del software instalados en los diferentes equipos y la razón de su instalación y uso, así como verificar las licencias y el vencimiento de las mismas; igualmente soporte debe informar ante cualquier mal uso del software y el vencimiento de las licencias para las respectivas acciones preventivas.

7.3.18. Administración remota

Para el uso de la red inalámbrica se debe tener en cuenta los siguientes requerimientos:

a. Aquellos que cuenten con dispositivos remotos y deseen conectarse con las redes inalámbricas de la empresa. deben hacerlo contando con los requerimientos y condiciones establecidas por la organización.
b. Solo el personal de soporte técnico administrará las redes inalámbricas y permitirá el acceso a dicha redes, según las claves y contraseñas determinadas.
c. Los dispositivos móviles tales como: pc, celulares, Smartphone y otros, con los cuales se puede intercambiar información, serán sincronizados únicamente con la autorización de soporte técnico y para uso exclusivo de las funciones propias de la organización.
d. Aplicativos de administración remota como vnc y escritorio remoto serán utilizados solo para los equipos conectados a la red interna de la organización.
e. Aplicativos de acceso remoto externo como TeamViewer, logmein, Radmin, deben ser autorizados previamente por el oficial de seguridad.
f. El acceso a los equipos de forma externa, se debe habilitar mediante reglas en el Firewall y con claves de seguridad que cumplan con los requisitos mínimos.

7.3.19. Control de acceso físico

El entorno físico es fundamental para el resguardo y custodia de la información.

a. El ingreso y salida de las instalaciones de la empresa se realizará mediante dispositivo biométrico y/o el carné con chip que lo identifica como miembro de la organización.
b. El carnet deberá portarse en un lugar visible durante el tiempo que permanezca en las instalaciones y/o para los casos de reuniones externas que de alguna manera representen a la organización.
c. Para el ingreso de terceros a la empresa es necesario la autorización desde la portería, identificando dependencia a la que desea ingresar; quién autorizará al personal ajeno a la organización al ingreso.
d. Todas las dependencias que refieran con información sensible o crítica debe contar con medidas de restricción para su acceso, de tal forma que el ingreso a tales lugares se realiza con previa autorización del dueño del proceso o líder de área y con los procedimientos de seguridad requeridos.
e. Los cuartos de cableado y centros de cómputo deberán contar con los requerimientos medio ambientales necesarios para proteger y cuidar la información como extintores, ups, lejos de posibles inundaciones, con aire acondicionado.
f. La empresa., para evitar e impedir el daño de la información por cortes de energía en lo equipos, regulará la corriente por UPS y conectara los equipos que considere a esta red.
g. Para el ingreso a los equipos debe existir un protocolo o procedimiento, que permita exclusivamente la entrada a miembros de la organización; en caso de terceros dicho ingreso debe realizarse con autorización del equipo de soporte técnico.

7.3.20. Escritorio y pantalla limpia

Uno de los elementos fundamentales para resguardar el proteger la información, es la de generar una cultura de cuidado con su espacio inmediato; por lo tanto:

a. Todos los miembros de la organización, deben tener su escritorio limpio y no consumir bebidas o comidas cerca de los equipos de cómputo
b. Toda información que se encuentra en físico, sea esta general, crítica o delicada, debe estar siempre bajo llave en los escritorios o archivadores destinados para su custodia. El acceso a ella debe seguir los procedimientos o protocolos de seguridad.
c. La información crítica y delicada, que se encuentre en los equipos de cómputo o de forma digital, debe ser archivada en carpetas con clave de acceso, las cuales están creadas en un servidor central para cada uno de los usuarios. El usuario de cada carpeta es responsable de subir la información delicada y crítica al servido.

7.3.21. Protección de los equipos

En la empresa la protección física y ubicación adecuada de los equipos es fundamental para evitar riesgos y minimizar pérdidas de la información

a. Los equipos de cómputo, estaciones de trabajo, telefonía, UPS, servidores, plantas telefónicas, portátiles, dispositivos de almacenamiento y cualquier equipo que almacene información o se considere importante para el desarrollo de la empresa, deberán ubicarse en un lugar amplio, protegido contra incendio, de daños medioambientales y contar con las condiciones de seguridad requerida por las normas existentes.
b. La empresa. cuenta con extintores necesarios de cada tipo y con planes de evacuación y prevención de riesgos de daños en caso de situaciones de riesgo.
c. Dado los servicios que presta la empresa., varios equipos de cómputo y, medios removible, deben ser sacados de la empresa; por ello, para su salida se debe registrar protocolos de egreso y contar con un seguro contra robo, en estos equipos no debe almacenarse información crítica o delicada.

7.3.22. Protección contra software malicioso

Para la protección de software malicioso en la empresa se realizan los siguientes requerimientos de seguridad:

a. Todos los recursos informáticos serán protegidos contra cualquier amenaza de daño por software malicioso; a través de un antivirus debidamente licenciado y que proteja contra cualquier ataque maligno.
b. Ninguno de los miembros de la organización, podrá descargar antivirus no autorizados y sin licencia legal
c. Ninguno de los miembros de la organización, estará autorizado para inhabilitar el antivirus corporativo o hacer uso de este de forma inadecuada.
d. Cada vez que se ingrese un dispositivo móvil al equipo de cómputo, deberá realizar la revisión del mismo con el antivirus instalado por la empresa.
e. Soporte técnico realizará controles y auditorias permanentes a los equipos de cómputo, para revisar las actualizaciones del antivirus y verificar el funcionamiento correcto del mismo.

7.3.23. Copias de respaldo

Toda la información que se considere crítica o delicada debe ser guardada o archivada en copias de respaldo, lo que impedirá incidentes de la información.

a. Cada usuario subirá a la carpeta del servidor -cuyo nombre es el mismo del usuario del dominio-, toda la información crítica que él maneje localmente y que considera se debe resguardar, a dicha información se le realizará un backup cada quince días a cargo de soporte técnico.
b. El backup generado es recogido cada quince días por la empresa encargada de resguardarlos.

c. Cada dueño de proceso es responsable de verificar que la información crítica y sensible de cada uno de los miembros del equipo, sea subida al servidor, a través de copias de seguridad en forma manual.

7.3.24. Medios removibles

El uso de los medios removibles, tales como: usb, cd, dvd y demás para el almacenamiento de información, será autorizado por soporte técnico, contando con los protocolos de seguridad y previo análisis de software malicioso con el antivirus corporativo.

7.3.25. Eliminación segura de la información

La eliminación de información sensible en medios físicos como documentos serán eliminados mediante pica papel, mientras que la información almacenada en medios como dvd, cds serán almacenados por el área administrativa hasta alcanzar un volumen considerable para realizar la destrucción mediante incineración. Para apoyar la gestión de limpieza y eliminación se información en los equipos de la organización, se realizará un procedimiento automático que realice estas tareas de mantenimiento de forma programada.

7.3.26. Comunicaciones sobre incidentes

La comunicación en caso de incidentes en la seguridad de la información, es de vital importancia para la solución y acción correctiva oportuna; por ello se establece:

- Cualquier incidente que ponga en riesgo o comprometa de alguna manera la información de la organización debe ser reportado de inmediato al comité de seguridad, o al oficial de seguridad en caso de que no se encuentren los miembros del comité. Si de igual manera no se encuentra alguno de ellos, se deberá transmitir el incidente observado al dueño del proceso.
- Es responsabilidad y un deber de cada uno de los colaboradores de la organización velar por el buen uso de la información y de manejar buenas prácticas contribuyendo a una mejora continua en el sistema de seguridad de la información.

7.3.27. Registro de fallas

Las fallas que se presenten en el SGSI, se deben registrar, documentar y analizar, tomando las medidas apropiadas para la acción correctiva.

El comité de seguridad de la empresa., será el primero en ser informado ante cualquier falla y será este estamento el encargado de establecer su revisión, solución y evaluar el impacto de la misma.

Igualmente, el comité de seguridad bajo el liderazgo del oficial, realizará los controles y auditorias necesarias para evitar nuevas fallas en el sistema.

7.3.28. Procedimientos de manejo de la información

Cada uno de los dueños de los procesos y según la matriz de activos de la información establecerá los procedimientos necesarios para el manejo de la información, teniendo en cuenta la clasificación establecida por la presente política. Los procedimientos serán evaluados y asesorados por el comité de seguridad de la información y aprobados por la Alta Dirección.

7.3.29. Procedimientos en caso de incidentes

Todos los incidentes deben ser reportados, descritos y detallados de manera escrita, se llevara una trazabilidad del mismo para reducir al máximo el impacto.

El oficial de la seguridad de la información, será el encargado de hacer los respectivos seguimientos al incidente y documentar para el comité de seguridad los resultados de las acciones correctivas.

7.3.30. Gestión del riesgo

Para la empresa, asumir la gestión del riesgo[30] en seguridad de la información, es de vital importancia; en este sentido el oficial de la seguridad, debe estar constantemente actualizando el inventario de activos y evaluando el nivel de criticidad de los mismos.

Para ello el oficial, utilizará lo establecido por la norma ISO 27001 y 27005[31], que establece las directrices necesarias de la gestión del riesgo, contando con el mapa de riesgos (ver anexo No. 5), elaborado para la empresa y que determina los riegos de la información crítica y los controles para minimizar dichos riesgos y ejecutar las acciones preventivas necesarias para gestar la seguridad en los activos de la información de la empresa.

[30] En el proceso de desarrollo del presente trabajo, se realizó un estudio de las diversas metodologías diseñadas para la gestión del riesgo, tales como; Magerit en sus diversas versiones, que se encuentra diseñado de manera originaria como metodología de gestión del riesgo y que aparece antes de la norma 27005. 2. y demás, pero debido a que la empresa es pequeña el comité de seguridad de la información determinó optar por realizar un mapa de riesgos de la información basado en la norma ISO 27005, que permitiera el desarrollo de la política y la prevención de incidentes de seguridad.

[31] ISO/IEC 27005:2008 proporciona directrices para la gestión de riesgos de seguridad de la información. Esto apoya los conceptos generales especificados en ISO/IEC 27001 y ha sido diseñada para ayudar a la puesta en práctica satisfactoria del análisis y la gestión del riesgo, fase principal del diseño de todo buen sistema de gestión de la seguridad de la información (SGSI). El conocimiento de los conceptos, modelos, procesos y terminologías descritas en ISO/IEC 27001 e ISO/IEC 27002 es importante para lograr el entendimiento completo de la ISO/IEC 27005:2008. ISO/IEC 27005:2008 es aplicable a todos los tipos de organizaciones (p.ej. sociedades mercantiles, administraciones públicas, organizaciones no lucrativas) que tengan la intención de manejar los riesgos que podrían comprometer la seguridad de la información de la organización. Esta norma actualiza a la antigua ISO 13335, partes 3 y 4. Recuperado de http://sgsi-iso27001.blogspot.com.ar/2008/06/publicada-la-iso-270052008-sobre-gestin.html septiembre de 2013.

7.3.31. Excepciones

Las excepciones a cualquiera de los lineamientos señalados por la actual política de seguridad de la información, serán determinadas por la Alta Dirección, previo informe del comité de seguridad, que después de analizar las condiciones de excepción a los lineamientos de la política, las remitirán a Alta Dirección para su aprobación.

7.3.32. Consideraciones finales

La presente política empezará a regir a partir de enero de 2014, cuya responsabilidad de auditoría y control le compete al comité de seguridad, quienes también se reunirán una vez por mes para evaluar el impacto de la política y documentar las excepciones a la misma.

Los dueños de proceso serán los encargados de cumplir y hacer cumplir, los lineamientos, procesos y procedimientos que se generen a partir de la presente política, notificando al comité de seguridad cualquier falla o anomalía al respecto.

7.4. EVALUACIÓN DE LA IMPLEMENTACIÓN DE LA METODOLOGÍA DE GENERACIÓN DE POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL GRUPO NYQUIST EN EL CASO DE LA EMPRESA DE SERVICIOS EN TELECOMUNICACIONES

La implementación de la metodología de generación de política de seguridad de la información, en el caso específico de la empresa de servicios en Telecomunicaciones, ubicada en la ciudad de Bogotá, se ejecutó siguiendo la metodología del grupo Nyquist, así:

1. En lo que respecta al ***planear***

Según lo ofrecido por la metodología del grupo Nyquist, la primera parte en el planear consistía en la elección del líder del proyecto y del oficial de la seguridad, proceso que se llevó a cabo completamente según las indicaciones de la metodología y elegido por quién recomendaba la misma.

El siguiente paso se relaciona con la creación del proyecto para la generación de la política y sus correspondientes procedimientos, que debía ser liderado por el oficial de seguridad de la información; como se muestra en el capítulo 2 de este proyecto de grado. La propuesta se diseñó llevando paso a paso cada una de las indicaciones, tal como definir los recursos humanos, económicos, el alcance y el cronograma de la propuesta.

Igualmente, se gestionó ante la alta gerencia tal como lo indica la metodología, la inscripción y aprobación del proyecto y de los recursos presupuestales y humanos necesarios para llevar a cabo el proyecto para la generación de la política de seguridad de la información. Es importante señalar que el proyecto se diseña con un alcance solo de la política, los procedimientos responden a otro proceso que surge de este proyecto pero que no son el objetivo primario.

Según la metodología del grupo Nyquist, se debía proseguir con la elección del comité de seguridad de la información y con los grupos de trabajo, en lo que respecta a la elección del comité se realizó según las indicaciones de la metodología, pero en lo que concierne a los grupos de trabajo, no se eligieron debido a que la empresa solo cuenta con 22 funcionarios en todas las áreas; de esta manera el comité se encargó de desarrollar todas las funciones de diseño, planeación y ejecución de la política de seguridad de la información. De la misma forma se definieron roles y funciones, teniendo en cuenta que las funciones y roles de los subgrupos que manifiesta la metodología se asignaron al comité y a los miembros de éste.

El comité de seguridad realizó la revisión del proyecto y lo ajustó según algunas recomendaciones, para proceder a su aprobación por parte de la alta dirección,

procedimiento que se realiza en concordancia con lo manifestado por la metodología del grupo Nyquist.

Según lo presupuestado por la metodología se procede a gestionar ante la alta dirección una primera jornada de capacitación por parte del oficial de seguridad, sobre los siguientes temas: Seguridad de la Información, cumplimiento de la normatividad legal vigente y la norma ISO 27001, controles de acceso, organización de la seguridad de la información, seguridad de los recursos humanos, seguridad física y del entorno; que no son todos los señalados por la metodología, pero si corresponden a un 60% de ellos, los otros recomendados por la metodología se trabajaron en jornadas de capacitación a posteriori.

A partir de entrevistas con cada uno de los dueños de los procesos, tal como lo señala la metodología se organizó el inventario de activos y el mapa de riesgos (no la matriz) y el formato para la política y lineamientos, estos tres fueron los únicos insumos de esta parte del proceso realizado, siguiendo la metodología del grupo Nyquist, pues lo que se refiere a la normatividad aplicable, procesos asociados al flujo de información, no se aplicaron para la generación de la política de seguridad de la información en el caso de la empresa de telecomunicaciones en la ciudad de Bogotá D.C.

Porcentaje de aplicabilidad del ***planear*** en la generación de la política de seguridad de la información en el caso de la empresa de telecomunicaciones en la ciudad de Bogotá D.C. es de un ***90%***

2. En lo que respecta al ***hacer***

En este aspecto, es necesario iniciar señalando, que el presente proyecto tiene como alcance solo la definición de la política y sus lineamientos, en lo que respecta a los procedimientos, corresponde a un proceso posterior para la certificación en ISO 27000; dicho esto en lo que concierne al hacer, se ejecuta el

paso a paso de la metodología generada por el grupo Nyquist, en lo que se acerca a la generación de la política.

Es necesario recordar que no se realizaron subgrupos de trabajo, por el tamaño en recursos humanos de la empresa; de tal forma que el comité se organiza con representantes de cada una de las áreas; así todo aquello que la metodología señala para ser realizado por los subgrupos, lo ejecuta el comité de seguridad de la información. El hacer corresponde al capítulo 3 del presente informe final.

Se analizaron cada uno de los insumos presentados en las entrevistas con los dueños de los procesos, y el inventario de activos de la información, al igual que le mapa de riesgos, clasificando y analizando dichos insumos; por parte del comité de seguridad para iniciar a redactar la política de seguridad; tal como lo señala la metodología ofrecida por el grupo Nyquist.

Luego de revisar los insumos el comité formuló el primer borrador de la política con sus respectivos lineamientos y algunos de los controles para la política, posteriormente se socializó con cada uno de los miembros de la empresa -en este apartado se evita todo lo concerniente al trabajo en los subgrupo por lo señalado anteriormente-, después de la socialización aparecen algunos comentarios, sugerencias y recomendaciones de algunos miembros de la organización, que permiten ajustar la política desde el comité de seguridad, este es el primer ajuste a la política.

Se procede con dicha política ajustada a entregarla a la alta dirección, quiénes realizan sus propias recomendaciones y correcciones, se procede a realizar los ajustes pertinentes.

Posteriormente, es enviado el documento para la aprobación final por la alta dirección y se instruye el proceso de capacitación y sensibilización con cada uno de las áreas y miembros de la empresa.

Todo lo concerniente a los procedimientos correspondientes a la política, solo se enuncian pero no son desarrollados, como lo indica la metodología del grupo

Nyquist; esto principalmente porque no es el alcance del proyecto y no incumbe al presente trabajo; aunque la mayoría de ellos quedan señalados en la política. De tal manera que los aspectos sobre procedimientos que se señalan en la metodología no fueron llevados a cabo.

En lo que respecta a la socialización y sensibilización frente a la política, se definen las estrategias y el cronograma para las mismas; igualmente la política, lineamientos y controles es publicada, tal como reposa en el capítulo 3 del presente informe final, política que es presentada oficialmente ante toda la organización para iniciar los procedimientos y su implementación.

Las jornadas de capacitación y sensibilización se ejecutan de acuerdo al cronograma, permitiendo afianzar una cultura de seguridad de la información.

Porcentaje de aplicabilidad del ***Hacer*** en la generación de la política de seguridad de la información en el caso de la empresa de telecomunicaciones en la ciudad de Bogotá D.C. es de un ***80%***

3. En lo que respecta al ***verificar:***

Según lo establecido anteriormente, el oficial de seguridad de la información Verifica los entregables de cada una de las etapas de la metodología y genera listado de pendientes, que son entregados al comité de seguridad, que informa que ya están todos los insumos solicitados.

Con ayuda de la encuesta de evaluación que reposa en el capítulo 5 del presente informe, se mide el grado de apropiación de la política y sus procedimientos en el personal y en los involucrados y se establecen los requerimientos de reinducción de personal e involucrados, en especial a aquellos que ingresan nuevos a la organización.

En lo que respecta a realizar los procesos de revisión de la política y sus procedimientos según los tiempos establecidos por cada una de ellas y con base en las condiciones organizacionales y de normatividad, no corresponde al presente trabajo este alcance, este hace parte del proceso de la empresa para la certificación en seguridad de la información; igualmente en lo que respecta a establecer un consolidado de requerimientos de actualización.

Porcentaje de aplicabilidad del ***Verificar*** en la generación de la política de seguridad de la información en el caso de la empresa de telecomunicaciones en la ciudad de Bogotá D.C. es de un ***60%***

4. En lo que respecta al ***actuar:***

En lo que respecta al ***actuar*** propuesto por la metodología del grupo Nyquist, se llevó a cabo lo concerniente a ejecutar las actividades necesarias para obtener los entregables pendientes, los cuales fueron adjudicados en su totalidad, pues la empresa es pequeña en procesos y personal, lo que hace más fácil la verificación por parte del oficial; igualmente se ejecutaron procesos de capacitación orientados a la reinducción de personal y de los nuevos integrantes del grupo, y finalmente en lo que respecta a actualizar la política y sus procedimientos con base en los requerimientos de actualización, el comité de seguridad realiza y realizará reuniones periódicas con el fin de llevar a cabo dichas actualizaciones, según los nuevos requerimientos normativos, legales o de exigencia de los clientes.

Porcentaje de aplicabilidad del ***Actuar*** en la generación de la política de seguridad de la información en el caso de la empresa de telecomunicaciones en la ciudad de Bogotá D.C. es de un ***80%***

En este sentido, el porcentaje de aplicabilidad de la metodología para la generación de una política de seguridad de la información por parte del grupo de investigación Nyquist, se aplicó así

1. En el planear un 90%
2. En el hacer un 80%
3. En el verificar un 60%
4. En el actuar un 80%

Con un total de un 77.5%

En el que se comprueba la importancia de la metodología para la generación de una política de seguridad de la información.

En lo concerniente a su aplicabilidad es eficiente y eficaz, debido al paso a paso para llevar a término la política; sin embargo en el planear existen algunos pasos demás, debido quizás a que la empresa dónde se aplica en este trabajo es pequeña.

Lo que no se llevó a cabo de la metodología presentada por el grupo Nyquist:

1. En el ***planear*** no se desarrollaron los subgrupos para la elaboración de insumos y la definición de la política; toda vez que la empresa cuenta con un personal reducido; igualmente no se realizaron tantas revisiones y borradores de la política, ya que solo fueron dos los preliminares de la política, evitándose el numero amplio de reuniones y encuentros que señalaba la metodología, porque siendo una empresa pequeña los miembros del comité son los líderes de los procesos y parte de la alta dirección.

   Las capacitaciones fueron programadas y realizadas según sugerencia de la metodología del grupo Nyquist y se convirtieron en la parte más importante del proceso, pues de esta forma se está consolidando una cultura de seguridad de la información en la empresa.

2. En el ***hacer*** la ruta fue clara y ejecutada en casi su totalidad, se evitó los procedimientos, por considerar que el alcance del proyecto no era este y porque la metodología no los ofrecía de manera clara; en este aspecto solo se siguieron las pautas para desarrollar, lineamientos y controles, que se establecen en la misma política. Se espera continuar con los procedimientos más adelante para llegar a la certificación.
3. En el ***verificar*** no se realizó la revisión de los procedimientos, porque como se señaló anteriormente no se contaba con ellos y los requerimientos de actualización se espera que con el paso del tiempo y algunas exigencias de los clientes, el comité realicé dicha actualización. La metodología es clara en este verificar; sin embrago, se considera que corresponde a un posteriori que no compete al presente informe.
4. En el ***actuar*** se realizaron las capacitaciones de reinducción y al personal nuevo, se verificaron la entrega de insumos faltantes, esperando la actualización de la política, según algunas condiciones que el paso del tiempo determinará.

La metodología del grupo Nyquist, fue determinante para el logro de la política de seguridad en el caso de la empresa de estudio, sin embargo por ser tan pequeña poseía algunos pasos de revisión, de formulación y consolidación de grupo, que no tenían cabida por lo reducido del personal y que agotaban mucho tiempo; de resto es pertinente señalar que dicha metodología contribuyo significativamente para consolidar no solo la política, sino gestar un proceso de cultura de seguridad de la información.

7.5. APLICACIÓN DE LA METODOLOGÍA DE GESTIÓN DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN, EN LA EMPRESA.

Existen varias metodologías de gestión del riesgo, que a lo largo de estas últimas décadas han sido utilizadas por diversas organizaciones, para evidenciar los

peligros que se pueden presentar en las empresas y de esta manera evitar incidentes que afecten y dificulten los procesos internos.

Es necesario en primera instancia aclarar el concepto de la gestión de riesgos de seguridad de la información, que se entiende como la forma en que una empresa analiza, clasifica, reduce y controla las posibles amenazas en cuanto a la información, para evitar los peligro latentes que puedan ocasionar daños a la empresa y sus terceros; lo anterior demuestra la importancia de establecer dentro de las organizaciones una metodología que permita a través de instrumentos y/o herramientas identificar la información crítica, revisar las causas de los riesgos y mantener en constante monitoreo dicha información, de tal forma que se evite incidentes y complicaciones al respecto que puedan alterar el buen funcionamiento de los procesos.

La norma ISO 27000, 27002 y 27005 presentan algunos conceptos claves que deben ser tenidos en cuenta para la comprensión de la gestión de riesgos:

Amenaza: causa potencial de un incidente no deseado, la cual puede causar daño a un sistema u organización. (ISO/IEC 27002:2005)

Vulnerabilidad: debilidad de un activo o grupo de activos, que puede ser explotada por una o más amenazas. (ISO/IEC 27002:2005)

Riesgo aceptable: decisión de aceptar el riesgo. (ISO/IEC 27001:2005)

Riesgo residual: riesgo remanente después del tratamiento del riesgo. (ISO/IEC 27001:2005)

Control: medio para manejar el riesgo; incluyendo políticas, procedimientos, lineamentos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal. (ISO/IEC 27002:2005)

Riesgo de seguridad de la información: el potencial de que una amenaza dada explote las vulnerabilidades de un activo o grupo de activos, causando pérdida o daño a la organización. (ISO/IEC 27008:2008)[32]

Desde lo anterior, se han observado entre otras las siguientes normas sobre la gestión del riesgo:

ISO 27005: esta norma contiene las recomendaciones y lineamientos necesarios para llevar establecer un sistema de gestión de riesgo de la información. La norma ofrece entre otros escenarios: identificación del riesgo, la evaluación del riesgo, análisis del riesgo, los lugares del riesgo y respuesta a los riesgos.

ISO 31000: su función principal es ayudar a las empresas sin importar lo grande o pequeñas que sean, a gestionar el riesgo con efectividad, a través de un número de principios que se instituyen en un (framework), este es un marco de trabajo para implementar la gestión de riegos en la cultura de calidad de la empresa, en todos y cada uno de los niveles.

Igualmente, estas son algunas de las metodologías de la gestión del riesgo, tenidas en cuenta por la empresa., para su estudio y evaluación, que permita realizar la elección más conveniente tomando como referencia que la empresa es pequeña, pero en crecimiento:

MAGERIT: esta metodología es desarrollada por el Consejo Superior de Administración Electrónica del gobierno de España, de todas las metodologías es la más complejas y detalladas.

La metodología MAGERIT, posee en su más reciente versión tres libros, el primero de ellos es un ejercicio teórico-conceptual sobre el riesgo, el segundo corresponde al catálogo de elementos y el tercero es la guía técnica para la implementación de la metodología.

[32] Información recuperada de http://www.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-de-la-informacin, septiembre de 2013.

La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza.[33]

OCTAVE: se centra en el estudio de riesgos organizacionales, principalmente en los aspectos relacionados con el día a día de las empresas. La evaluación inicia a partir de la identificación de los activos relacionados con la información, definiendo este concepto con los elementos de TI que representan valor para la empresa (sistemas de información, software, archivos físicos o magnéticos, personas). De esta forma, OCTAVE estudia la infraestructura de información y, más importante aún, la manera como dicha infraestructura se usa. Se considera que, con el fin de que una organización pueda cumplir su misión, los empleados de todos los niveles necesitan entender qué activos relacionados con la información son importantes y cómo deben protegerlos[34].

OCTAVE se centra principalmente en organizar un buen equipo de trabajo que se encuentre compuesto por miembros de todas las dependencias de la organización, situación que permitirá identificar con mayor facilidad los riesgos y potenciar las acciones preventivas y de mejora.

Para lo cual OCTAVE diseña tres procesos:

1. Construcción de perfiles de amenazas basadas en activos.
2. Identificación de vulnerabilidades en la infraestructura.
3. Desarrollo de estrategias y planes de seguridad.

FAIR: esta metodología es utilizada especialmente para complementar otras, pues permite realizar un análisis cualitativo de los riesgos existentes en la empresa.

---

[33] Información recuperada de septiembre de 2013. http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.U2_hA_l5Ooh.

[34] Información recuperada de http://www.uv.mx/universo/535/infgral/infgral_08.html septiembre de 2013.

TARA: esta metodología fue desarrollada por Intel y se preocupa fundamentalmente por establecer los controles en cada uno de los activos de la información, realizando el monitoreo constante a los mismos.

La metodología TARA incluye documentación de cambios a los controles y sistemas, la realización de análisis de impacto a los cambios asociados, y la premisa de informar sobre el estado de seguridad a los empleados o participantes de la organización (terceros) de una forma regular[35].

EBIOS: es una metodología francesa, que se compone de un número determinado de guías y una herramienta de código libre, con cinco fases organizadas de la siguiente manera:

Fase 1. Análisis del contexto, estudiando cuales son las dependencias de los procesos del negocio respecto a los sistemas de información.

Fases 2 y 3, Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto.

Fases 4 y 5, Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales[36].

En este sentido, la empresa., realiza al interior del comité de seguridad de la información, un estudio de la normatividad vigente sobre la gestión del riesgo y las diversas metodologías implementadas por las empresas y organizaciones, en miras de prevenir y evitar incidentes, realizando un proceso de evaluación, que conlleve a implementar la más adecuada para la organización y teniendo en cuenta que la empresa decidió elegir la metodología del grupo de investigación Nyquist, para la ejecución de una política de seguridad de la información.

Para la decisión de la metodología, se realiza el siguiente procedimiento:

---

[35] Información recuperada de http://www.slideshare.net/roberth.chavez/gestin-del-riesgos-de-seguridad-de-la-informacin, septiembre de 2013.

[36] Información recuperada de http://seguridadinformaticaufps.wikispaces.com/EBIOS+-+Metodologia+Francesa+Analisis+y+Gesti%C3%B3n+de+Riesgos, septiembre de 2013.

1. Presentación por parte del oficial de seguridad de la normatividad, métodos y metodologías de la gestión del riesgo.

2. Revisión y presentación del inventario de la información por el oficial de seguridad, a partir de las entrevistas realizadas a los dueños de los procesos.

3. Revisión de la política de seguridad y los controles de la misma

4. Discusión sobre las metodologías

5. Elección de la metodología teniendo en cuenta las necesidades de la empresa, pues se considera importante ubicar una metodología, que sea llevada de manera ágil y que no se constituya en una sobrecarga de funciones a los miembros de la organización.

Luego de la evaluación de cada una de las metodologías expuestas en el comité y con la asesoría del oficial de seguridad, dicho comité determina: no aplicar una metodología específica de las estudiadas, sino crear a partir de la norma 27005 y 31000, los procedimientos necesarios para llevar a término una adecuada gestión del riesgo en la empresa; toda vez que la política fue creada con la metodología del grupo Nyquist que se articula claramente a los procesos, pero estas de la gestión del riesgo operan más para empresas grandes por lo complejo de su implementación. (Ver anexo No. 2 acta del comité de seguridad)

De esta forma, la empresa., realiza en las siguientes fases en la gestión del riesgo de seguridad de la información:

Fase 1: Asignar al comité de seguridad de la información, cuyos integrantes son representativos de cada una de las áreas de la empresa, para establecer la matriz y el mapa de riesgos; al igual que monitorear y mantener vigentes los controles de la información.

Fase 2: Clasificación de los activos de la información en el nivel alto, medio y bajo de criticidad, a partir de evaluación con cada uno de los dueños de los procesos.

El nivel protección 1 corresponde al más alto y el 3 al más bajo; la relevancia corresponde al tipo de información, siendo 1 la más importante y crítica y la cinco la más baja.

Tabla 3: Inventario de activo con nivel de criticidad

DESCRIPCIÓN DEL ACTIVO	TIPO DE ACTIVO	NIVELES DE PROTECCIÓN	RELEVANCIA
Código Fuente (CTLog) Software propio	Software	1	1
Código Fuente (CTMail) Software propio	Software	1	1
Código Fuente (CTMessage) Software propio	Software	1	1
Instaladores	Software	1	1
Código Fuente (CTLog) Software propio	Software	1	1
Código Fuente (CTMail) Software propio	Software	1	1
Código Fuente (Dali) Software propio	Software	1	1
Código Fuente (CTMessage) Software propio	Software	1	1
Código Fuente (IVR) Software propio	Software	1	1
Instaladores y licencias del Software empresarial(Microsoft)	Archivos	2	2
Acta de reuniones	Documentos	3	4
Acta de requerimientos	Documentos	2	3
Scripts SQL	Software	3	3
Instaladores Bases de Datos	Software	1	1
Manuales de productos	Documentos	3	4
Indicadores	Documentos	2	3
Diseños Bases de datos		1	1
Backup Generales (Instaladores de los productos, instaladores bases de datos, codigo fuente, bases de datos de los aplicativos manejados en la empresa, información designada por cada usuario para este fin).	Software	1	1
Cronograma de mantenimiento de los equipos	Documentos	3	4
Hojas de vida de las equipos (Servidores, PCs, portátiles, planta telefónica)	Documentos	3	4
CRM	Software	2	3
Cronograma de soporte para los equipos físicos	Documentos	3	4

Contratos de soporte	Documentos	3	3
Cotizaciones	Documentos	1	1
Actas de entrega	Documentos	3	3
Acuerdos	Documentos	2	3
Lista de Clientes	Documentos	2	3
Lista de precios	Documentos	1	1
Ventas	Documentos	1	3
Órdenes de Compra	Documentos	1	3
Documentación de los proyectos	Documentos	2	3
Facturas	Documentos	1	3
Lista de canales	Documentos	1	3
Convenios con canales y/o clientes	Documentos	1	3
Contratos con clientes	Documentos	1	3
indicadores	Documentos	2	3
Brochures	Documentos	3	3
Datashit	Documentos	3	4
Página Empresarial	Software	2	3
Publicidad	Software	3	4
Redes sociales	Software	3	4
Balances	Documentos	1	1
Certificados	Documentos	2	3
Nomina	Documentos	1	1
Impuestos	Documentos	1	1
Documentos Legales	Documentos	1	1
Reportes ante la Dian	Documentos	1	1
Información DANE	Documentos	1	1
Conciliaciones bancarias	Documentos	1	1
Hojas de vida de los miembros de la organización	Documentos	2	3
Contratos laborales	Documentos	1	3
Formatos ISO	Documentos	2	3
Inventario de activos	Documentos	3	4
Dali	Software	2	3
CTMail	Software	2	3
CTLog	Software	2	3
Antivirus AVG	Software	2	3
Office	Software	2	3
Windows	Software	2	3
Sql Server	Software	2	3
Compras	Documentos	2	3
Visual Studio	Software	2	3

PCs	Hardware	2	3
Portátiles	Hardware	2	3
Servidores	Hardware	1	2
Impresora	Hardware	2	3
Disco Duro USB	Hardware	2	3
Kit Vcam Completo	Hardware	2	3
Celulares	Hardware	2	3
Moden	Hardware	2	3
IMG	Hardware	2	3
Plantas telefónicas	Hardware	1	3
Teléfonos IP	Hardware	2	3
Teléfonos digitales	Hardware	2	3
Hub 24 puertos	Hardware	2	3
UPS	Hardware	2	3
Inventario de PBX Telefónicas	Hardware	2	2
Inventario de Teléfonos IP	Hardware	2	2

Fuente: Autor
Referencia: entrevistas con los dueños de los procesos de la empresa.

Fase 3: Elaboración de un mapa de riegos que identifique luego de evaluación con los dueños del proceso y evaluada la clasificación de activos por su nivel de protección y relevancia, las amenazas, riesgos y controles pertinentes para evitar incidentes con la seguridad de la información.

Tabla 4: Mapa de Riesgos de la empresa.

AMENAZA	RIESGO				CONTROLES		
Descripción	Descripción	Tipo de Riego			Descripción	Preventivo	Correctivo
		Alto	Medio	Bajo			
Ingresos no autorizados a equipos de la empresa mediante software de conexión remota.	Hurto, pérdida o alteración de la información.		x		Realizar conexión remota mediante un sistema que tenga las políticas de seguridad de la empresa.	x	
Bajas de energía y apagones eléctricos	Perdida de información actual (la que está siendo consultada o modificada en el momento). Daño en equipo físico.	x			Realizar revisión de la red eléctrica para pasar los PCs con información crítica a una corriente regulada por UPS. Adquirir una UPS con mayor capacidad.	x	Envió a técnico interno o externo para el diagnóstico y posible relación de la parte física.

Ataques de ingeniería social	Dar a conocer información de alta relevancia a terceros.	x			Realizar capacitaciones iniciales o dar a conocer de manera puntual, práctica y sencilla las políticas y el proceso de seguridad de la información en la empresa. Programar retroalimentaciones periódicas.	x	
Virus informáticos	Amenazas a la integridad, disponibilidad y confidencialidad de la información.		x		Actualización centralizada de antivirus empresarial. Política sobre el escaneo de memorias usb o dispositivos externos. Políticas sobre el ingreso a páginas	x	

					sospechosas		
Usuarios del sistema con poco conocimiento de la información sensible o crítica de la empresa	Eliminar, modificar información sin ser conscientes de la relevancia que esta tiene.		x		Capacitación a personal nuevo sobre las políticas de seguridad de la información de la empresa. Validar los perfiles de cada miembro de la empresa para que estén acordes a las funciones del mismo dentro de la organización. Proteger los documentos de alto impacto con algún tipo de clave.	x	

Incendios o inundaciones	Perdida de información física como documentos impresos en papel. Daños en equipos de cómputo.		x		Revisión de la red de agua y alcantarillado para identificar posibles fugas. Contratar con un tercero el almacenamiento de equipos. Contar con sensores de humo. Extintor apropiado en un área estratégica.	x	
Ingresos no autorizados a personal ajeno a la empresa	Robo de dispositivos móviles o equipos de cómputo. Riesgo contra la confidencialidad de la información.		x		Política de ingreso seguro al personal ajeno a la empresa. Dispositivo físico para controlar el ingreso a las	x	Validación con cámaras de seguridad del edificio, para tratar de identificar el caso.

					instalaciones.		
Robo de equipos fuera de la empresa	- Perdida del recurso físico de la empresa. - Perdida de información sensible de la organización.	x			Seguro contra robo para los equipos que estén dispuestos a salir de la empresa. Evitar guardar información de lata relevancia en estos equipos. Los equipos destinados a este proceso, se deben proteger con contraseña segura para el ingreso al sistema operativo.	x	Denuncio a las autoridades correspondientes.

Falta de conocimiento y falta de apropiación del sistema de seguridad de la información por parte del empleado.	No identificar la información de alta relevancia. No realizar el trámite adecuado ante algún incidente de seguridad de la información.	x			Dar una información precisa, práctica y puntual de la seguridad de la información de la organización. Realizar retroalimentación periódica.	x	
Daño en equipos locales por algún suceso externo o interno.	Perdida de gran contenido de información.	x			Guardar la información de alta relevancia en el servidor central de forma diaria, para reducir la cantidad de información que se puede dañar.	x	
Robo o uso inadecuado de información por personal interno de la organización	Hurto de información por personal de la organización.	x			Definir de forma clara y precisa en los contratos laborales las cláusulas		

					contractuales sobre el uso adecuado de la información de la organización.		

Fuente: Autor
Referencia: entrevistas con los dueños de los procesos de la empresa.

Fase 4: Implementación de los controles en la política de seguridad, dada las pautas de la metodología del grupo de investigación Nyquist, se realizó la política de seguridad de la información con los respectivos controles que son parte de la gestión de riesgo y resultado de la evaluación, tanto del proceso de la elaboración de la política como del mapa de riesgos.

Fase 5: Verificación de los riesgos residuales, después de tratados los riesgos, al empresa la empresa., establece que para aquellos riesgos que son remanentes después de realizado el control y la acción respectiva; es necesario que el comité de seguridad, busque estrategias para minimizar impactos posteriores y lo establezca en la política de seguridad de la información.

A partir de estas fases la organización implementa la gestión de riesgos y constituye un nivel de satisfacción al respecto, luego de las respectivas jornadas de capacitación y sensibilización, que informaron al personal en general como se encuentra la empresa en lo que respecta a los activos de la información, su nivel de protección, relevancia y criticidad

Aunque no se estableció y validó una metodología existente, si se operó con ayuda de la metodología del grupo Nyquist y de las normas existentes en gestión del riesgo, lo que permitió una organización y conocimiento claro por parte de la empresa de la situación de la información y cómo procedimentalmente llevar a cabo los controles y medidas preventivas y correctivas al respecto.

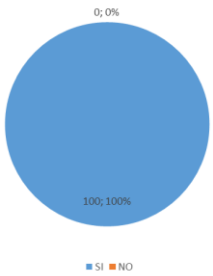
7.6. EVALUACIÓN DE LA IMPLEMENTACIÓN DE LA METODOLOGÍA DE GENERACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN EN LA EMPRESA.

Luego de aprobada la política de seguridad de la información por la Alta Dirección y realizada su socialización ante la organización, implementando

controles, se evalúa su incidencia en la cultura organizacional, encontrando los siguientes hallazgos[37]:

1. Existe una nueva cultura con respecto a la seguridad de la información, generada desde las jornadas de sensibilización y capacitación realizadas por el oficial y comité de seguridad de la información. La política fue socializada a todos y cada uno de los miembros de la empresa, quienes aportaron algunos elementos a partir de sus funciones y experiencias.
2. El incremento del porcentaje de conocimiento por parte los miembros de la empresa con respecto al el sistema Seguridad de la Información ha incrementado significativamente.
3. De tal manera, se puede apreciar un mayor sentido de pertenencia por el tema de seguridad de la información, sensibilizándose sobre la importancia de proteger sus activos.

Grafico 41: Conocimientos sobre Seguridad de la Información



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

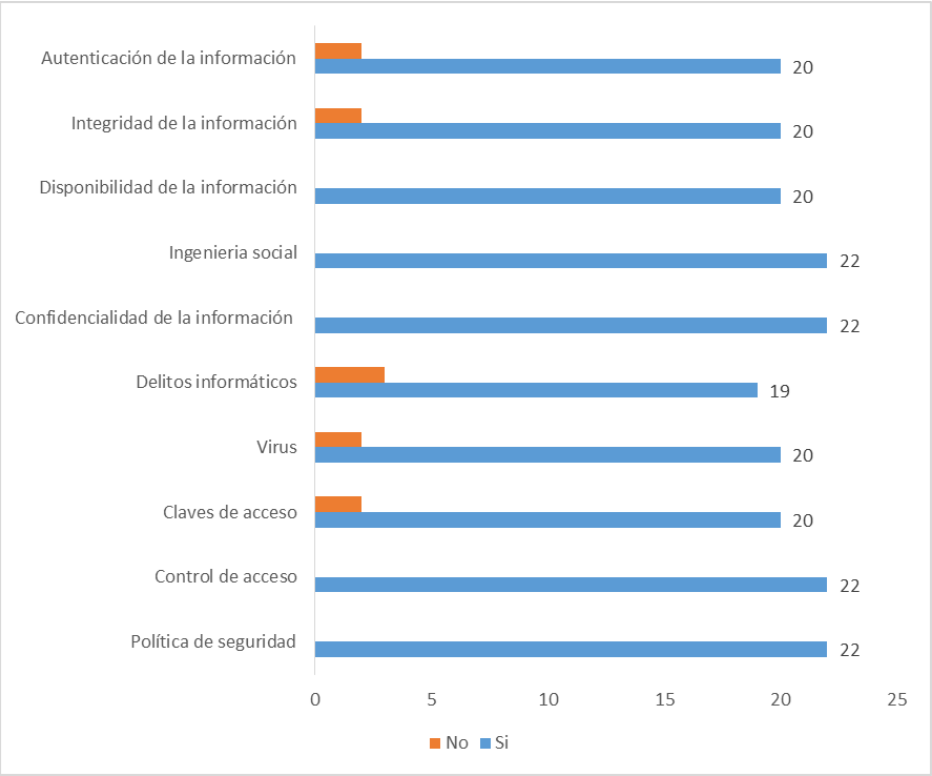
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

[37]Los hallazgos de evaluación, son el resultado de la aplicación nuevamente de la encuesta de diagnóstico implementada para el primer objetivo de la presente investigación, y que se realiza después de las jornadas de capacitación y sensibilización; al igual que de la socialización de la política de seguridad de la información aprobada por la Alta Dirección.

Existe un aumento significativo en la comprensión alrededor de la pregunta ¿conoce usted qué es la seguridad de la información?, en el diagnostico el 98% daban una respuesta afirmativa, ahora luego de las jornadas de capacitación y sensibilización, el total de la empresa sabe lo que es la seguridad de la información y no solo los del área de ingeniería; situación muy significativa, porque permite generar un ambiente de prevención y cuidado con los activos de información.

Grafico 42: Conocimientos específicos de Seguridad de la Información



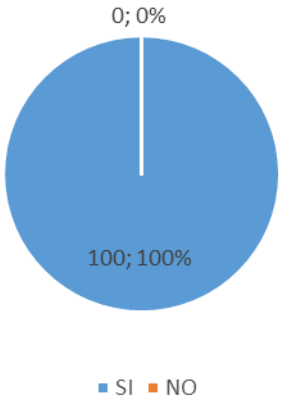
PREGUNTA	ENCUESTADOS RESPUESTA SI	PORCENTAJE
Política de seguridad	22	100%
Control de acceso	20	91%
Claves de acceso	18	82%
Virus	20	91%
Delitos informáticos	21	95%
Confidencialidad de la información	19	86%
Ingeniería social	18	82%
Disponibilidad de la información	20	91%
Integridad de la información	20	91%
Autenticación de la información	18	82%

Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Luego de las capacitaciones y las jornadas de sensibilización, la comprensión sobre seguridad de la información se estableció en un plano menos superficial, ya que los miembros de la organización empiezan a utilizar términos más especializados y a conocer a profundidad el manejo del sistema; al igual que a tomar conciencia de la importancia de proteger los activos de la información. Por ello, en la encuesta de evaluación el porcentaje de conocimientos sobre temas específicos de seguridad de la información se eleva con respecto a la prueba de diagnóstico, y se evidencia una relación de estos conceptos en el plano operativo de cada uno de los funcionarios.

Grafico 43: Capacitación sobre Seguridad de la Información



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

Fuente: Autor

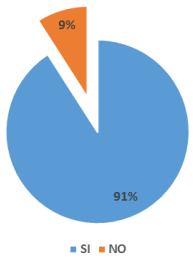
Referencia: Encuesta de evaluación (marzo de 2014)

Continuando, antes se evidenciaba un 0% de capacitación sobre seguridad de la información a los funcionarios, ahora el 100% de ellos ha recibido capacitación sobre el sistema, según los requerimientos y las necesidades de

la organización y no solo esto sino que al interior de la empresa se han realizado jornadas de sensibilización sobre el cuidado y protección de los activos de la información.

Estas jornadas de capacitación y sensibilización, se han realizado según lo establecido por la metodología para la generación de la política de seguridad de la información, del grupo Nyquist; todas ellas con el objetivo y propósito de las generar una cultura y cuidado de la protección de los activos de la información y de establecer responsabilidades particulares para el funcionamiento del sistema.

Grafico 44: Confidencialidad en Seguridad de la Información al ingreso a la empresa

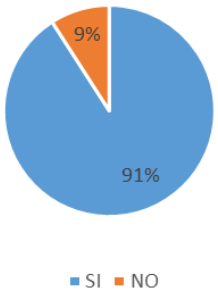


RESPUESTA	ENCUESTADO	PORCENTAJE
SI	20	91%
NO	2	9%

Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Grafico 45: Contrato de confidencialidad



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	20	91%
NO	2	9%

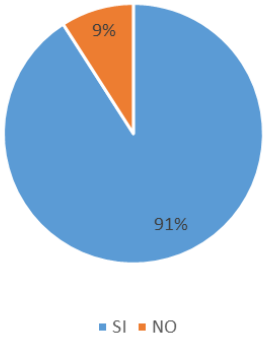
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

En lo que respecta, a la confidencialidad de la información al ingreso de la empresa y en los contratos, se realiza la revisión de los mismos en los que claramente se posee dicha cláusula, pero que no era conocida por la totalidad de los miembros de la empresa, así que en una de las jornadas de capacitación se informa a los funcionarios sobre la cláusula de confidencialidad y las penalidades que conlleva el incumplimiento, esta información permite sensibilizar sobre la responsabilidad de la información y el cuidado que se debe tener con la que cada uno de los funcionarios maneja.

La relectura de los contratos, generó un impacto positivo permitiendo comprender la importancia de realizar los procedimientos de seguridad del sistema y la razón de hacerlos correctamente.

Grafico 46: Correo institucional

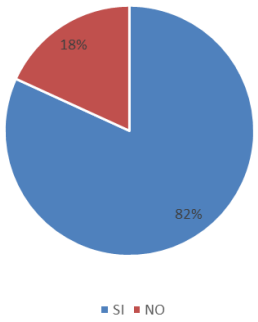


RESPUESTA	ENCUESTADO	PORCENTAJE
SI	20	91%
NO	2	9%

Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Grafico 47: Seguridad contraseña del correo electrónico



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	18	82%
NO	4	18%

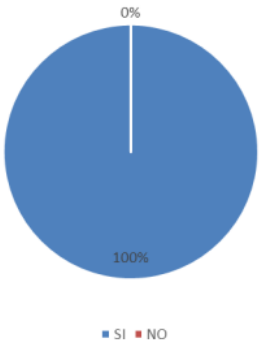
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

En lo relativo, al correo electrónico y la contraseña de seguridad del mismo, es importante destacar que en la encuesta de diagnóstico el 77% de los funcionarios poseían correo y el 55% de ellos tenían una clave segura con códigos alfa numéricos, que asegurará la privacidad de la información y el resguardo de la misma.

En la encuesta de evaluación se observa un aumento en la seguridad de la contraseña del correo electrónico, ya que en una de las jornadas de capacitación se sensibiliza a los funcionarios sobre el tema, indicando lo que al respecto refiere la política de seguridad de la información.

Grafico 48: Portar los instintivos de seguridad



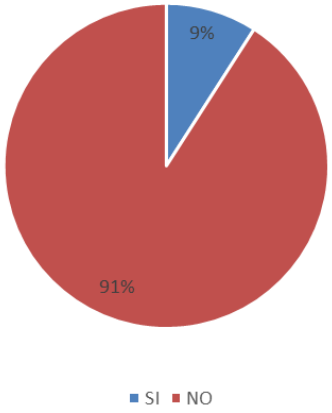
RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Las jornadas de sensibilización, permitieron incentivar el porte de distintivos de la empresa, que a pesar de ser pequeña y que todos los miembros se conocen entre sí, es necesario portar las credenciales, para el ingreso en la portería principal y en especial para el reconocimiento de terceros y el cuidado que con ellos se debe tener.

Grafico 49: Acceso a los activos de Seguridad de la Información



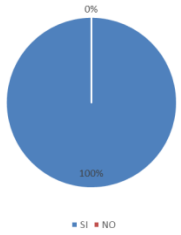
RESPUESTA	ENCUESTADO	PORCENTAJE
SI	2	9%
NO	20	91%

Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Uno de los aspectos más importantes de mejora, que se ha tenido en la empresa, es el que se observa al respecto del libre acceso de la información; ya que con la aplicación de la política de seguridad implementada, no existe libre acceso a la información para todos los miembros, sino se crean niveles de acceso y en ello solo el 9% de los funcionarios posee acceso total y libre de la información; mejora importante si se tiene en cuenta que antes de entrar en funcionamiento la política el 50% de los miembros poseía libre acceso, situación que podría generar incidente y fugas de información para la organización.

Grafico 50: Eliminación segura de la información



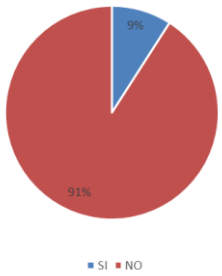
RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

En lo que respecta, a la eliminación segura de la información, en el resultado de la encuesta diagnóstica solo el 14% de los usuarios conoce el procedimiento; pero después de la socialización de la política, el 100% de los funcionarios conocen el manera de eliminar de forma segura la información; situación que permite minimizar riesgos y evitar situaciones críticas.

Grafico 51: Información guardada en dispositivos personales



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	2	9%
NO	20	91%

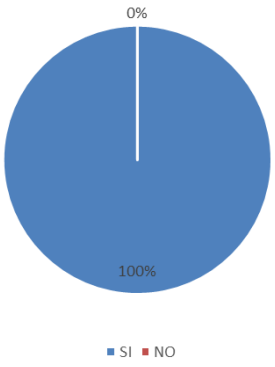
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

La información de la empresa guardada en dispositivos personales ha disminuido significativamente, tomando en cuenta la sensibilización al respecto en las jornadas creadas para este y otros temas; de tal manera que de un 36% de funcionarios que guardaban información de la empresa en sus dispositivos personales, se pasó al 9% de ellos.

Lo que permite minimizar riesgos e ir generando conciencia al respecto, para llegar al 100% de funcionarios que no realicen este tipo de procesos y ejecuten los lineamientos de la política para este tipo de situaciones.

Grafico 52: Conocimiento del antivirus de la empresa



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

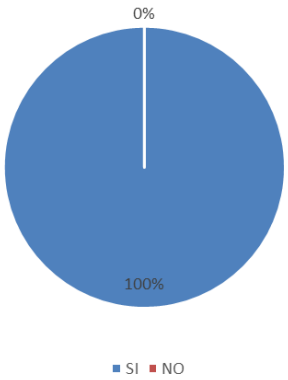
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

En la encuesta diagnóstica el 91% de los usuarios conocían sobre el antivirus corporativo, a partir de los procesos de capacitación el 100% de los funcionarios conocen no solo el tipo de antivirus, sino el manejo de actualización y otras políticas al respecto, como no desinstalarlos, que hacen parte de los lineamientos de seguridad; de la misma, forma se concientiza a los

funcionarios del antivirus de vital importancia para preservar los activos de la información.

Grafico 53: Restricción al personal ajeno a la organización



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

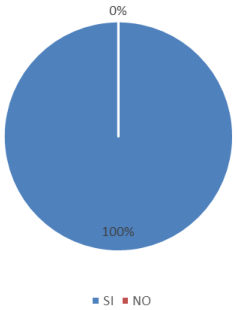
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

En lo pertinente a los procesos relacionados con la restricción al ingreso, de personal ajeno a la organización, en la encuesta diagnóstica se evidencia que el 82% del personal conocía el proceso, pero después de la socialización de la política, el 100% de los usuarios conocen el proceso.

Igualmente, se espera que además de conocer el proceso, los funcionarios lo apliquen con todos y cada uno de los visitantes, guardando el registro de llegada, salida, la razón y motivo de la visita; al igual que la dependencia que visita.

Grafico 54: Autenticación de usuarios al ingreso de la información

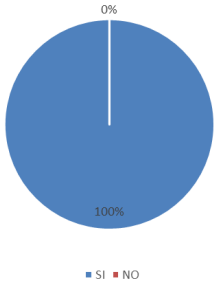


RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Grafico 55: Conocimiento de procedimientos de documentación



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

Fuente: Autor

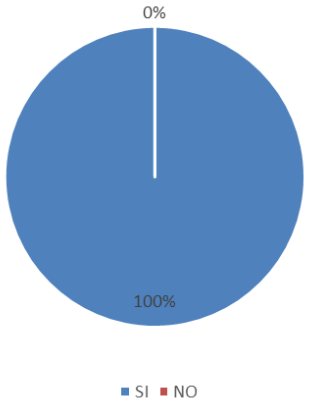
Referencia: Encuesta de evaluación (marzo de 2014)

En lo que respecta al conocimiento de los usuarios sobre los procedimientos del sistema, en la encuesta de inicio el conocimiento es del 38%, después de

socialización y capacitación sobre la política de seguridad de la información, los miembros de la organización reconocen los procedimientos y controles del sistema.

Sin embargo, el conocimiento no significa la aplicación, la empresa se encuentra en jornadas de sensibilización que motive a la rigurosidad en la ejecución de los procedimientos y se eviten fallas e incidentes de la seguridad.

Grafico 56: Acceso restringido a las páginas de internet de la empresa



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

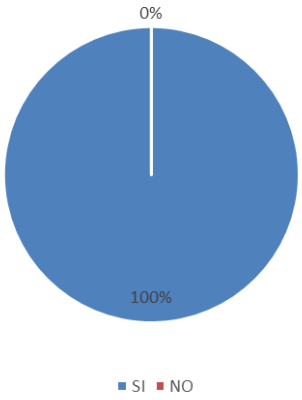
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Este es uno de los aspectos en los que más ha cambiado la organización, ya que en el diagnóstico solo el 9% conocía sobre las restricciones a ciertas páginas web, después de la socialización de la política, el 100% conocen las páginas que la empresa ha determinado como restringidas y el uso que debe dársele a algunas páginas, que aunque no son restringidas -tales como las redes sociales- debido a que pueden ser utilizadas como medio de difusión y publicidad de la empresa, se deben utilizar de manera prudente y segura .

De la misma manera, que en otros ítems no solo con el conocer sobre determinado aspecto de la política, significa que está se encuentre en ejecución; por ello la importancia de las jornadas de sensibilización y la motivación por parte de los dueños de los procesos o jefes de área a cada uno de los miembros de la organización.

Grafico 57: Capacitación de ataques de prevención de ataques informáticos



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

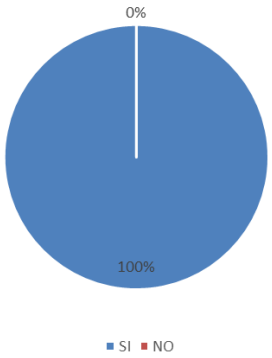
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

La encuesta diagnóstico muestra que el 0% de los miembros de la empresa habían recibido capacitación sobre ataques informáticos, situación que cambió considerablemente ya que el 100% de los encuestados informa una jornada de capacitación sobre ataques informáticos; capacitación que espera mitigar daños por este tipo de incidentes.

Se espera realizar aún más capacitaciones al respecto y mantener informados a los miembros de la organización de los nuevos virus y amenazas que circulan por la red.

Grafico 58: Capacitación de usuarios y contraseñas



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	0%

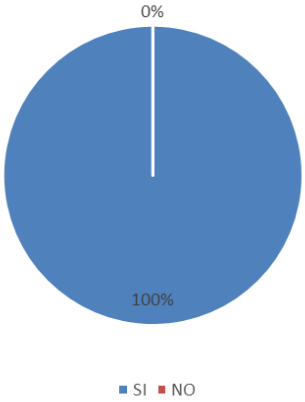
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Igualmente, los miembros de la organización han recibido en los últimos meses en el marco de la socialización de la política pública, capacitación de usuarios, aspectos de contraseña segura e ingreso al sistema, al igual que manejo de dispositivos móviles y guarda de información en carpetas en el servidor de datos para su protección; capacitación que antes solo era dada al 9% de los funcionarios y que al día de hoy se cuenta con el 100% de ellos capacitados e informados.

Los anteriores controles permiten asegurar la información y evitar riesgos por el mal uso de los usuarios; es importante mantener constantemente la capacitación a los funcionarios que permita el sostenimiento del sistema.

Grafico 59: Conoce la política de la seguridad



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	100%

Fuente: Autor

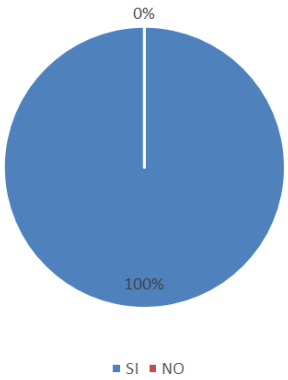
Referencia: Encuesta de evaluación (marzo de 2014)

En la jornada socialización realizada a todos y cada uno de los miembros de la organización, de la política de seguridad de la información, jornada en la que se establecieron compromisos y se sensibilizó a la comunidad sobre la importancia de asumir con responsabilidad los lineamientos y controles establecidos. La política fue enviada a los correos institucionales de cada uno de los miembros, para su relectura y apropiación.

Esto indica que aunque se debe realizar nuevas socializaciones y capacitaciones sobre la misma, ya existe un conocimiento claro de la política y se espera cumplir con su apropiación, generando una cultura de la seguridad de la información.

De este modo, se pasa de un 45%, al 100% del conocimiento de la política de seguridad; es importante aclarar que ese 45% conocían un documento que no era la política, sino un lineamiento establecido para cumplir con cliente.

Grafico 60: Capacitación y socialización de la política de Seguridad de la Información



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	100%

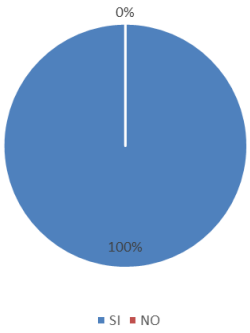
Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Se han realizado capacitaciones sobre diversos lineamientos y controles de la política de seguridad de la empresa; de la misma forma se han realizado jornadas de sensibilización a través de ejercicios pedagógicos, que permitan generar un espíritu de compromiso y responsabilidad con los activos de la información

Son necesarias más capacitaciones y establecer algunos procedimientos para ser socializados, pero el proceso se encuentra en una fase de consolidación que va por buen camino; por ello se pasa de 5% a un 100% en el conocimiento y socialización de la política.

Grafico 61: Conoce los encargados de la Seguridad de la Información

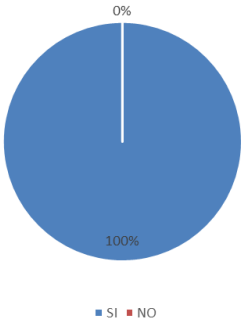


RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	100%

Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Grafico 62: la Idoneidad del personal encargado de la Seguridad de Información



RESPUESTA	ENCUESTADO	PORCENTAJE
SI	22	100%
NO	0	100%

Fuente: Autor

Referencia: Encuesta de evaluación (marzo de 2014)

Durante las capacitaciones se informó a toda la comunidad, sobre quiénes eran los responsables de la política y en general de la seguridad de la información, señalando cargos, funciones, roles, compromisos y formación para ejercer dicha responsabilidad.

Promoviendo una cultura del compromiso, durante la socialización se aclara que no existe un único responsable, sino un equipo y que de una u otra forma todos hacen parte de la seguridad de la información.

A través de un esquema se presenta el oficial, comité, el sponsor aclarando funciones y alcance de la misma. Se señala la responsabilidad de los dueños de los procesos y de los demás miembros de la organización, al ser una empresa pequeña se detectan rápidamente los roles y las funciones.

En estas nuevas responsabilidades y exposición del grupo líder del proceso se aumenta de un 63% de conocimiento al 100% sobre los responsables de la seguridad de la información.

Es importante aclarar, que antes no existían cargos establecidos, sino que era una persona quien realizaba gestiones alrededor del tema, generalmente para cumplir necesidades de ciertos clientes; por ello, cuando se habla en la encuesta de diagnóstico del conocimiento del personal de un 63% de los responsables de la seguridad, no se refiere a un equipo organizado y que cumpliera los requerimientos de la norma, sino a la persona que respondía ante ciertos clientes sobre el tema.

Después de realizado el análisis de evaluación sobre la implementación de la política de seguridad de la información, se puede establecer algunas conclusiones que dan cuenta tanto de la metodología generada por el grupo Nyquist, como de la situación en la empresa, sobre la seguridad de la información.

Es importante antes de dar paso a las conclusiones, observar que la empresa gracias a la implementación de una política de seguridad de la información y de la gestión de riesgos, ha establecido criterios claros sobre el manejo y atención

a la información en los niveles de acceso y criticidad, permitiendo de esta manera que las condiciones de protección de la información sean los necesarios para que los procesos funcionen con eficacia y eficiencia.

En ese sentido, se puede observar como cambios trascendentales en beneficio de la empresa en cuanto a seguridad se refiere, los siguientes:

1. Existe un inventario de los activos de la información, que antes del proceso no había, permitiendo reconocer en cada uno de los procesos que maneja la empresa, la información relacionada con ellos, lo que establece para los dueños de los procesos la claridad de la información que tienen a su cargo y la responsabilidad en el manejo de ella.
2. La clasificación de la información según su criticidad, explicada en la matriz de riesgo, que se realizó en el marco de este trabajo de grado para la empresa. permitió de manera significativa identificar la información crítica que se maneja en cada proceso, para establecer en la política de seguridad los procedimientos y controles necesarios, que impidan una posible falla, fuga e incidente de seguridad, situación que fue de un gran avance para la empresa y que para los dueños de procesos y en general para los miembros de la organización es uno de los elementos más importantes para gestar un SGSI y a la vez proteger a la empresa de incidentes que la perjudiquen.
3. Capacitar al recurso humano de la empresa sobre la seguridad de la información y más allá de proteger sensibilizar, es otro de los elementos importantes que se lograron con la realización de este proceso, ya que es el inicio de gestar una cultura de seguridad de la información, que se constituye en el fin último del sistema.
4. Consolidar un equipo de trabajo que fortalezca las necesidades del sistema de seguridad de la información, lidere los procesos alrededor del tema y proponga alternativas de actualización y verificación, es uno de los avances significativos desde la primera evaluación hasta la conclusión del proceso.
5. Por último, la consolidación de la política de seguridad de la información de la empresa, siguiendo paso a paso la metodología presentada por el grupo

Nyquist, permitió consolidar un diseño de seguridad de la información y establecer los procedimientos y controles necesarios, para evitar riesgo y gestar acciones preventivas en lo relativo a la información.

De lo anterior, se observa un avance significativo en la empresa. en lo relativo a seguridad de la información, debido a que antes de iniciar este proceso no se contaba con un equipo consolidado para este tema, el personal de la organización conocía poco sobre el tema y la importancia de cada uno de ellos para la protección de la información, no se contaba con el inventario de activos, ni con matriz de riesgos, no se poseía una política definida con sus respectivos controles y procedimientos.

Situación que permite entrever la validación del proceso y los resultados obtenidos a partir del mismo, para que la empresa. consolide su propio Sistema de Gestión de Seguridad de la Información.

En el escenario de la validación de la hipótesis

La hipótesis que se planteó en la presente investigación, fue: “La aplicación de las metodologías de generación de política y de gestión de riesgos mejorará la seguridad de la información en la empresa”

De este modo, se pudo comprobar a través de la aplicación de la encuesta final después de la creación de la política de seguridad y la metodología de gestión de riesgo que:

La aplicación de las metodologías de generación de política y de gestión de riesgos mejoró la seguridad de la información en la empresa. porque:

1. Los miembros de la empresa en un 100% fueron capacitados en lo que se refiere a la normatividad de asociada a la gestión del riesgo y política de seguridad de la información, conociéndose que al principio de la presente de investigación solo conocían sobre el tema el 15%.
2. El 100% de los miembros de la empresa reconocen claramente que la política de seguridad de la información de la empresa. conociéndose que

al inicio de la presente investigación no existía una política de seguridad de la información definida y clara

3. El 100% de los miembros conocen y manejan vocabularios, nociones y categorías relacionadas con la seguridad de la información, conociéndose que al inicio de la presente investigación solo el 15% de los miembros conocían algo relacionado con la seguridad de la información.
4. El 100% de los usuarios conocen las páginas restringidas de la empresa y por consiguiente no las visitan, situación que al inicio de la investigación solo era conocido por el 9%
5. El 100% de los miembros de la empresa conocen los procedimientos necesarios para mantener la seguridad de la información en la organización, situación que permite evitar incidentes y generar confianza con los terceros, clientes y demás.
6. El 98% de los miembros ya no guarda la información en los dispositivos personales, el restante 2% corresponde a personal autorizado y lo hace bajo el estricto cumplimiento de la política al respecto; situación que permite evidenciar un mejoramiento significativo, pues este era uno de los riesgos más inminentes de la empresa.
7. La empresa tiene claro el nivel de criticidad y la relevancia de la información, el 100% de los dueños de los procesos conocen los procedimientos indicados por la matriz de riesgos y la política de seguridad de la información según el nivel de la información.
8. El mapa de riesgos constituye un instrumento importante para prevenir y actuar ante una situación de riego. Y es conocido y socializado en el 100% de los miembros de la organización.
9. Existe claramente conformado un grupo encargado para la seguridad de la información y que se encuentra integrado por representantes de las diferentes dependencias.
10. Existen responsables de mantener actualizado tanto el inventario, como el mapa de riesgos; el 100% de los miembros de la empresa conocen a

dichos responsables e informarán sobre cualquier modificación del inventario.

Del mismo modo, existen otros aspectos cualitativos que permiten validar la hipótesis del mejoramiento de la seguridad de la información en la empresa., después de aplicar la metodología de generación de una política de seguridad de la información por el grupo Nyquist.

1. El paso a paso dado por la metodología, permite establecer un orden lógico y participativo por parte de los miembros de la empresa, constituyendo de manera clara roles y responsabilidades.
2. Las referencias normativas y legales a las que hace referencia la metodología, permiten instituir un marco teórico consistente en el que los responsables de la seguridad, pueden hacer uso.
3. Los formatos creados para realizar los lineamientos son funcionales, pertinentes y permiten la organización de los procesos.
4. Al establecer la forma de realizar las entrevistas y organizar la matriz, se facilita de manera sustancial la redacción y organización de la política.
5. La implementación de la metodología a través del ciclo PHVA, genera orden e indica acciones concretas a seguir.
6. Las indicaciones para la construcción de la política proporcionan eficacia en el momento de la redacción.
7. La metodología abarca más allá que la redacción de la política, también su implementación y la consolidación de una cultura de seguridad de la información, que la hace pertinente y relevante.
8. Algunos pasos pueden evitarse, pues se sobrentienden en el ejercicio y parece que se repiten, como los señalados en el capítulo tres. En este aspecto la conformación de subgrupo es imposible en una empresa pequeña como en esta, lo mismo que la revalidación de la política por tantas instancias, ya que siendo pocos los miembros de la organización no es necesario el uso de tantos pasos; igualmente, todo aquello de verificar los insumos sobra, pues no se puede continuar en los procesos sin referir a ellos.

9. La política parece ser diseñada para empresas grandes que utilizan un grupo amplio de recurso humano, que empresas como la empresa, no posee, podrían hacerse algunas referencias de adaptación para empresas pequeñas o que hasta ahora se encuentren consolidándose en el mercado, y no solo en recurso humano, sino el planear y el hacer.
10. La metodología se adapta perfectamente a las exigencias de la ISO 27000 y su familia de normas, lo que puede ayudar a una certificación al respecto, luego de aplicar rigurosamente la metodología.
11. Las jornadas de capacitación y sensibilización son de suma importancia para el logro de los objetivos, su regularidad y eficacia han sido principal soporte para el éxito de la implementación de la política
12. Se da inicio al proceso para la consolidación de una cultura de seguridad de la información que permita reducir incidentes y fallos sobre el tema.
13. La asignación de funciones y roles dentro de la empresa, en lo relativo a la seguridad de la información, permite establecer criterios de valuación, seguimiento, auditoría y control del sistema.

Con una política clara y adecuada a las necesidades de la empresa, esta puede participar en licitaciones locales y nacionales, cuyas exigencias al respecto son imperativas.

CONCLUSIONES

En el escenario final del presente proyecto de investigación, se establecen como conclusiones las siguientes:

a. La empresa., al momento del primer diagnóstico contaba con dificultades disientes en lo que respecta al manejo y seguridad de la información tales como no contar con la claridad de los activos, falta de compromiso de los integrantes de la empresa, no contar con responsables y líderes que se encargaran de gestionar lo relacionado con la seguridad de la información, y ante todo la falta de conocimientos y capacitación del personal. Situación que la llevó a tener varios incidentes de seguridad de la información, siendo uno de ellos catalogado como de alto impacto para la organización; evidenciando de esta forma que era imperativo prestar atención a esta aspecto de manera urgente.

b. La metodología aplicada para la generación de una política de seguridad de la información dentro de la organización generada por el grupo de investigación de la Universidad Tecnológica de Pereira Nyquist, aunque requiere ajustes como hacer algunas referencias de adaptación para empresas pequeñas o que hasta ahora se encuentren consolidándose en el mercado, sobre todo en el planear y el hacer, permitió de una forma estructurada y clara, llevar el proceso de principio a fin con un resultado positivo para la organización luego del segundo diagnóstico realizado, donde se evidencia la capitación y concientización del personal, de vital importancia para una empresa pero que no eran tenidos en cuenta antes de la implementación de este proyecto.

c. La utilización de una metodología de gestión del riesgo basada en la norma 27005 y 31000 de ISO, dio como resultado una alta aceptabilidad por parte de la alta gerencia y de los dueños de proceso ya que identificaron sus activos, definieron su criticidad y relevancia y a partir de esto se evidencio claramente lo que requiere mayor atención dentro de la organización, aspectos como el ingreso biométrico a las instalaciones, la revisión de los perfiles de permisos a los usuarios, refuerzo en los acuerdos de confidencialidad, entre otros, fueron tenidos en cuenta y reforzados. Se pudo identificar las amenazas, canalizar los recursos y de esta manera dar una gestión adecuada a los riesgos.

d. Luego de realizado el diagnostico de los miembros de la empresa, posterior a la implantación de la política de seguridad de la información, es claro, según los resultados, que hay una mayor comprensión de lo que significa la seguridad de la información implementada en la empresa, en donde se identifican claramente unos líderes del proceso, así como los procedimientos implementados para tratar un posible incidente de seguridad. Se evidencia una concientización por parte de los colaboradores en aspectos como el uso adecuado de las redes sociales, el internet, los dispositivos externos, así como un conocimiento sobre los virus y sus posibles daños y los antivirus y las ventajas de su correcta utilización.

e. Una metodología para la generación de la política de seguridad de la información se hace necesaria para una implementación coherente, ágil y bien estructurada de la política de seguridad dentro de una organización, en especial en la pequeña y/o mediana empresa como la empresa, donde sustentar un consultor externo o el designar uno de sus colaboradores de tiempo completo para esta tarea sería demasiado costoso para ser considerado, incluso la falta de uno o dos

colaboradores por pocas horas se ve reflejado en la congestión dentro de su área, por lo anterior la metodología debe ser clara y los más puntual posible para optimizar el tiempo de implementación y reducir lo menos posible la alteración del servicio prestado por la empresa.

f. De tal forma, como se estableció en la validación de la hipótesis, la empresa. mejoró significativamente los procesos relacionados con seguridad de la información; toda vez que se implementa con eficiencia y eficacia cada uno los aspectos de la política, se establece el comité con sus respectivas funciones, existe un responsable o líder de la seguridad y en especial por la capacitación y sensibilización de los miembros de la organización, todo ello genera un clima organizacional proclive a mantener en funcionamiento la seguridad de la información y realizar procesos de gestión alrededor de ello. En síntesis la empresa mantiene un adecuada seguridad de la información y mejora continua en dicho proceso de gestión.

BIBLIOGRAFÍA

1. ACEITUNO CANAL, Vicente “Seguridad de la Información: expectativas, riesgos y técnicas de protección”.Ed Noriega Editores. México. D.F. 2006

2. ALMANZA JUNCO, Andrés Ricardo. “seguridad informática en Colombia. Tendencias 2011-2012” en Revista sistemas seguridad y privacidad y sistemas de información. No. 123 abril-junio de 2012. ISSN 0120-5919. Bogotá. Colombia

3. CALDER, Alan. “Nueve claves para el éxito. Una visión general de la implementación de la norma NTC-ISO/IEC 27001”. ICONTEC. Governance publishing. Bogotá, Colombia. 2006.

4. EBIOS 2010 - Expression des Besoins et Identification des Objectifs de Sécurité [Online] http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html. Recuperado julio de 2013.

5. HERNÁNDEZ SAMPIERI, R, FERNÁNDEZ COLLADO, C, BAPTISTA LUCIO, P. “Metodología de la investigación”. McGraw-Hill. México D.F. cuarta edición. 2006.

6. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Implementación del Sistema Gestión de Seguridad de la información. (ISO 27000).Bogotá: ICONTEC, 2009

7. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Requisitos del Sistema Seguridad de la Información. (ISO 27001).Bogotá: ICONTEC, 2005.

8. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Buenas prácticas y controles de la seguridad de la información. (ISO 27002).Bogotá: ICONTEC, 2007

9. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Guía para el desarrollo utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI. (ISO 27004).Bogotá: ICONTEC, 2009

10. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. directrices para la gestión del riesgo en la seguridad de la información. (ISO 27005).Bogotá: ICONTEC, 2011

11. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Risk management – Principles and guidelines, de la International Organization for Standardization (ISO 31000). Bogotá: ICONTEC, 2008.

12. Metodologías de Análisis de Riesgos [Online]- http://secugest.blogspot.com/2008/11/metodologias-de-analisis-de-riesgos.html. Recuperado julio de 2013.

13. MENDOZA, ROSENDO - "Sistema de gestión para la seguridad de la información - Caso: Centro de tecnología de información y comunicación" - República Bolivariana de Venezuela. [Online] http://www.slideshare.net/mmujica/mi-defensa. Recuperado julio de 2013.

14. ORTÍZ ANDRADE, Marcela. “Gestión de la información” en Revista Sistemas Inteligencia de negocios. No. 120 julio-septiembre de 2010. ISSN 0120-5919.Bogotá. Colombia.

ANEXOS

Anexo 1: Encuesta diagnóstico y evaluación

ENCUESTA A LOS MIEMBROS DE LA EMPRESA (_____)

SISTEMA GESTIÓN SEGURIDAD DE LA INFORMACIÓN

CARGO: _____

TIEMPO EN LA EMPRESA:

0-3 AÑOS ____ 4 A 6 AÑOS ____ 7 A 10 AÑOS ____ 10 AÑOS O MÁS ____

EDAD:

18 A 25 AÑOS ____ 26 A 35 AÑOS ____ 36 A 45 AÑOS ____ 46 AÑOS O MÁS ____

NIVEL DE ESCOLARIDAD:

BACHILLER ____ TÉCNICO ____ PROFESIONAL ____ POSTGRADO ____

La siguiente encuesta tiene por objetivo identificar los conocimientos de los miembros de la empresa en lo que respecta a la seguridad de la información; para ello es importante contar con su sinceridad y franqueza en la respuesta de los siguientes interrogantes:

No.	DESCRIPCIÓN	SI	NO	NS/NR
1.	¿Conoce usted qué es seguridad de la información?			
2.	¿Cuál de los siguientes términos conoce y/o maneja?			
	a. Política de seguridad			
	b. Control de acceso			
	c. Claves de acceso			
	d. Virus			
	e. Delitos informáticos			
	f. Confidencialidad de la información			
	g. Ingenieria social			
	h. Disponibilidad de la información			
	i. Integridad de la información			
	j. Autenticación de la información			
3.	¿Usted ha recibido en alguna oportunidad capacitación sobre seguridad de la información?			
4.	¿Al ingresar a la empresa recibió capacitación y/o inducción sobre seguridad de la información?			
5.	¿Al ingresar a la empresa recibió usted clave de acceso al sistema?			
6.	¿Al ingresar a la empresa le informaron sobre aspectos de confidencialidad de la información?			
7.	¿Recuerda usted haber firmado en el contrato clausulas sobre confidencialidad y/o buen uso de la informac			
8.	¿Cuenta usted con correo institucional?			
9.	¿Su clave de sistema cuenta con los requerimientos mínimos de seguridad? (más de 8 caracteres, contraseña alfanumérica, login diferente al password, etc)			
10.	¿Cuenta usted con carné y lo porta visiblemente para el acceso a la empresa?			
11.	¿Usted cuenta con libre acceso a toda la información de la empresa (documentos, archivos digitales, softwa			
12.	¿Conoce el proceso de eliminación segura de la información de la empresa?			
13.	¿Conoce usted algún incidente sobre seguridad de la información en la empresa?			
14.	¿Usted tiene documentos e información de la empresa en computadores y dispositivos personales?			
15.	¿Sabe usted si el computador que maneja en la empresa cuenta con antivirus?			
16.	¿Sabe usted si existe restricción de ingreso a la empresa de personal ajeno a la misma?			
17.	¿Conoce usted si existe algún procedimiento para la autenticación de usuarios en el ingrreso a la informació			
18.	sabe usted si existe un procedimiento documentado en la empresa para:			
	a. Apagar los equipos			
	b. Manejo de la información			
	c. Copias de respaldo			
19.	¿Sabe usted si existe acceso restringido a algunas páginas de internet en la empresa?			
20.	¿La empresa lo ha capacitado sobre la prevención de ataques informaticos o de virus?			
21.	¿En la empresa lo han capacitado para el manejo adecuado de los usuarios y contraseñas?			
22.	¿Utiliza usualmente los dispositivos USB para el traslado de información de la empresa?			
23.	¿Utiliza usted CD o DVD para el manejo y traslado de la información de la empresa?			
24.	¿Maneja usted información sensible de la empresa?			
25.	¿Sabe usted si existe una política de seguridad de la información en la empresa?			
	SOLO SI LA RESPUESTA EN LA PREGUNTA 25 ES SI, CONTINUE LA ENCUESTA	**SI**	**NO**	**NS/NR**
26.	¿Conoce usted la política de seguridad de la información en la empresa?			
27.	¿La empresa socializa constantemente la política de seguridad de la información con los miembros de la organización?			
28.	¿Conoce usted quiénes son las personas encargadas del manejo de la política de seguridad de la información en la empresa?			
29.	¿Sabe usted si el personal encargado de la seguridad de la inforrmación recibió la capacitación necesaria para el manejo de la misma?			
30.	¿Conoce el plan de contingencia del sistema de seguridad de la información en la empresa?			

Anexo 2: Actas de la alta dirección

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

FORMATO DE ACTAS Y SEGUIMIENTOS

Fecha: Agosto 02 del 2013	**No. Acta: 01**
Proyecto: Política de seguridad de la información	
Lugar: Instalaciones	
Participantes: Carlos Villamizar Johana Rodriguez Diego Fernando Nieto Guillermo Rodriguez	

Objetivo

Id	Descripción	Res
1	• Presentar el proyecto para la generación de una política de seguridad de la información y de gestión de riesgo para la aprobación de la misma por parte de la alta gerencia.	

Id	Descripción	Res
1	• Presentación del proyecto a la alta gerencia. • Definición del alcance del proyecto • Revisión y aprobación del proyecto por parte de la alta gerencia.	

Observaciones

Id	Descripción
	Realizar próxima reunión para designar el director del proyecto, líder del proyecto y miembros del comité de seguridad de la información.

Compromisos

Id	Descripción
	Reunión para la conformación de comité de seguridad de la información.

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

Firmas:

Carlos Villamizar

Johana Rodriguez

Diego Fernando Nieto

Guillermo Rodriguez Guillermo Rodriguez Gahara.

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

FORMATO DE ACTAS Y SEGUIMIENTOS

Fecha: Agosto 22 del 2013	**No. Acta: 02**
Proyecto: Política de seguridad de la información	
Lugar: Instalaciones	
Participantes: Carlos Villamizar Johana Rodriguez Diego Fernando Nieto Guillermo Rodriguez	

Objetivo

Id	Descripción	Res
1	• Se realiza reunión con cada dueño de proceso o persona designada por este para realizar la conformación del comité de seguridad de la información y asignar un líder y director del proyecto "Elaboración e implementación de una política de seguridad de la información".	

Id	Descripción	Res
1	• Se eligen los miembros del comité, procurando que cada proceso dentro de la empresa tenga un representante. • Se elige como el director del proyecto al ingeniero Mauricio Noguera basado en su experiencia y años en la empresa, además de ser él quien actualmente maneja lo referente a la seguridad de la información. • Como líder se nombra a Guillermo Rodríguez teniendo en cuenta que está desarrollando su trabajo de grado "Aplicación De Metodologías De Generación De Política Y De Gestión De Riesgos En Seguridad De La Información Como Caso De Estudio En La Empresa • A continuación se nombran los integrantes del comité de seguridad: Johana Rodriguez, Leidy Ortiz, Mauricio Noguera, Diego Nieto, Alexander Ortiz, Guillermo Rodriguez.	

Observaciones

Id	Descripción
	Miembros de comité: realizar reuniones, revisar, ajustar y aprobar los lineamientos que conformaran la Política de seguridad de la información, los cuales serán presentados por el líder del proyecto. Director del proyecto: Realizar acompañamiento en el proceso realizado por el líder del proyecto, durante la elaboración de los lineamientos que conformaran la política de seguridad de la

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

	información de la empresa. Líder del proyecto: Elaborar, los lineamientos para conformar la política de seguridad de la información en Calltech, además de realizar los ajustes indicados por el comité de seguridad de la información.

Compromisos

Id	Descripción
	Presentación del costo aproximado del proyecto por parte del líder del proyecto a la alta gerencia para su aprobación.

Firmas:

Carlos Villamizar

Johana Rodriguez

Diego Fernando Nieto

Guillermo Rodriguez Guillermo Rodriguez Bahara

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

FORMATO DE ACTAS Y SEGUIMIENTOS

Fecha: Septiembre 03 del 2013	**No. Acta: 03**
Proyecto: Política de seguridad de la información	
Lugar: Instalaciones _	
Participantes: Carlos Villamizar Johana Rodriguez Diego Fernando Nieto Guillermo Rodriguez	

Objetivo

Id	Descripción	Res
1	• Presentación del costo del proyecto, aprobación y destinación de recursos por la alta gerencia.	

Id	Descripción	Res
1	• Se presenta un cuadro detallado de los recursos necesarios para la elaboración del proyecto • Los tiempos presentados se dan de forma línea por cada participante incluyendo los tiempos de capacitación de los integrantes de la organización. • Se da un valor estimado a cada hora utilizada en la elaboración del proyecto. • La alta gerencia aprueba los tiempos y costos establecidos para el proyecto. •	

Observaciones

Id	Descripción
	Se debe socializar las generalidades del proyecto con los integrantes del comité de seguridad del a información, para dar por iniciado el proyecto

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

Id	Descripción
	Realizar reunión con los integrantes del comité de seguridad de la información, para plantear las generalidades del proyecto y dar por iniciado el mismo.

Firmas:

Carlos Villamizar

Johana Rodriguez

Diego Fernando Nieto

Guillermo Rodriguez Guillermo Rodriguez Galvis.

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

FORMATO DE ACTAS Y SEGUIMIENTOS

Fecha: Enero 09 del 2014	**No. Acta: 08**
Proyecto: Política de seguridad de la información	
Lugar: Instalaciones	
Participantes: Carlos Villamizar Johana Rodriguez Diego Fernando Nieto Mauricio Noguera Guillermo Rodriguez	

Objetivo

Id	Descripción	Res
1	• El oficial de seguridad de la información presentan la primera versión de la política de seguridad de la información a la Alta gerencia.	

Puntos tratados en la reunión

Id	Descripción	Res
1	• Presentación formal de la política de seguridad de la información a la alta gerencia. • Se presentan los aspectos relevantes del inventario de activos de seguridad de la información realizado. • La alta gerencia realiza las recomendaciones y ajustes a la política presentada.	

Compromisos

Id	Descripción
	Reunión para presentar la versión de la política de seguridad de la información con los ajustes indicados al comité de seguridad.

Observaciones

Id	Descripción

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

	No se realizaron observaciones al respecto.

Firmas:

Carlos Villamizar

Johana Rodriguez

Diego Fernando Nieto

Mauricio Noguera

Guillermo Rodriguez

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

FORMATO DE ACTAS Y SEGUIMIENTOS

Fecha: Enero 23 del 2014	**No. Acta: 09**
Proyecto: Política de seguridad de la información	
Lugar: Instalaciones	
Participantes: Carlos Villamizar Johana Rodriguez Diego Fernando Nieto Guillermo Rodriguez	

Objetivo

Id	Descripción	Res
1	• El oficial de seguridad de la información presentan la versión de la política de seguridad de la información con los ajustes indicados por la alta gerencia para su aprobación.	

Puntos tratados en la reunión

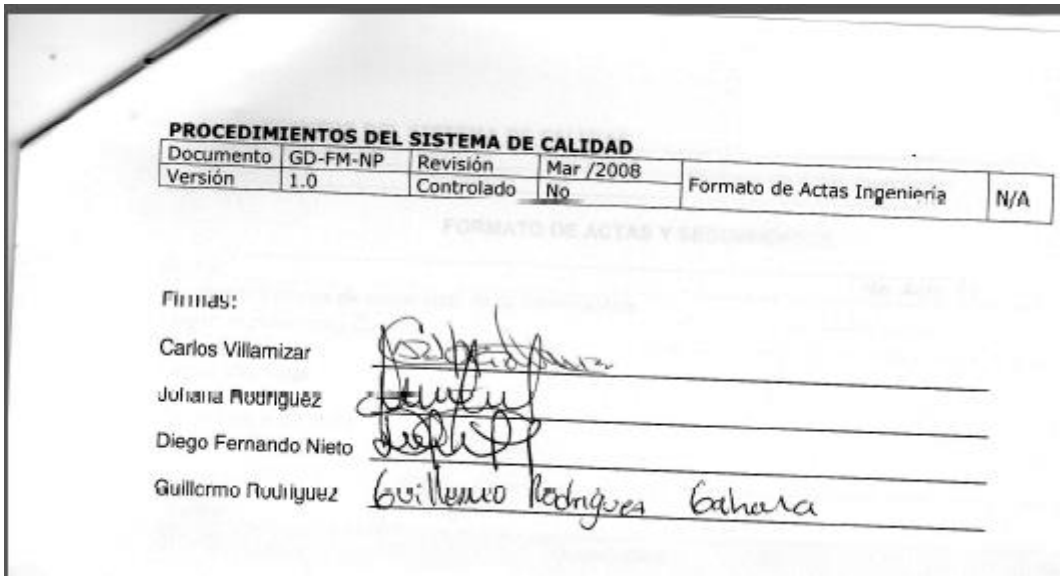
Id	Descripción	Res
1	• Se realiza la aprobación de la política de seguridad de la información de la empresa Calltech por parte de la alta gerencia.	

Compromisos

Id	Descripción
	Reunión para definir una forma de socialización que impacte al mínimo el proceso laboral de la organización, buscando que la socialización sea lo más puntual y practica posible.

Observaciones

Id	Descripción
	No se realizaron observaciones al respecto.



PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

Firmas:

Carlos Villamizar

Juliana Rodriguez

Diego Fernando Nieto

Guillermo Rodriguez Guillermo Rodrigues Cabrera

Anexo 3: Actas de comité de seguridad de la información

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

FORMATO DE ACTAS Y SEGUIMIENTOS

Fecha: Octubre 04 del 2013	**No. Acta: 04**
Proyecto: Política de seguridad de la información	
Lugar: Instalaciones	
Participantes: Johana Rodriguez Laura Triviño (Encargada) Mauricio Noguera Diego Nieto Alexander Ortiz Guillermo Rodriguez	

Objetivo

Id	Descripción	Res
1	• Presentación de las generalidades del proyecto • Capacitar al comité de seguridad de la información respecto a sus funciones dentro del proyecto. • Capacitar al comité de seguridad de la información sobre los temas básicos.	

Puntos tratados en la reunión

Id	Descripción	Res
1	• Que es seguridad de la información y su importancia en las empresas. • Descripción del proyecto a implementar y su alcance. • Funciones y responsabilidades de los integrantes del comité de seguridad de la información. • Beneficios de una política de seguridad de la información implementada en la empresa.	

Compromisos

Id	Descripción
	Presentar un primer borrador de la política de seguridad de la información al igual que presentar el cuadro de inventario de activos para ser tenido en cuenta para la gestión del riesgo.

Observaciones

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

Id	Descripción
	Reunión con el comité de seguridad para la presentación y aprobación de insumos necesarios para la generación de la política de seguridad de la información

Firmas:

Johana Rodriguez .....

Laura Triviño (E) ..... Laura Triviño

Mauricio Noguera .....

Diego Nieto .....

Alexander Ortiz .....

Guillermo Rodriguez ..... Guillermo Rodriguez Gahona.

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

FORMATO DE ACTAS Y SEGUIMIENTOS

Fecha: Octubre 17 del 2013	**No. Acta: 05**
Proyecto: Política de seguridad de la información	
Lugar: Instalaciones	
Participantes: Todos	

Objetivo

Id	Descripción	Res
1	• Brindar información general en lo relacionado con la seguridad de la información. • Presentación de los integrantes del comité de seguridad • Se presentan algunas formalidades del proyecto	

Descripción

Id	Descripción	Res
1	Toda la información se realiza enviando al correo electrónico y reforzando con cada usuario si se presenta alguna duda.	

Observaciones

Id	Descripción
	Presentar la política de seguridad a la Alta Gerencia, luego de realizados los ajustes del comité.

Compromisos

Id	Descripción
	NA

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.U	Controlado	No		

Observaciones

Id	Descripción
	Realizar los ajustes en los insumos según los ajustes indicados por los dueños de proceso

Compromisos

Id	Descripción
	Reunión para presentar la primera versión de la política de seguridad de la información al comité de seguridad.

Firmas:

Jehana Rodriguez .....

Laura Triviño (e) .....

Mauricio Noguera .....

Diego Nieto .....

Alexander Ortiz .....

Guillermo Rodriguez .....

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

FORMATO DE ACTAS Y SEGUIMIENTOS

Fecha: Diciembre 12 del 2013	**No. Acta: 06**
Proyecto: Política de seguridad de la información	
Lugar: Instalaciones	
Participantes: Johana Rodriguez Laura Triviño (Encargada) Mauricio Noguera Diego Nieto Alexander Ortiz Guillermo Rodriguez	

Objetivo

Id	Descripción	Res
1	• El oficial de seguridad de la información presenta los insumos (matriz de riesgos de seguridad de la información y el inventario de la información, esquema de criticidad de la información), que serán utilizados para la generación de una política de seguridad de la información.	

Puntos tratados en la reunión

Id	Descripción	Res
1	• Formato para el inventario de los activos. Se realiza la presentación del inventario de activos realizado, después de entrevista con cada uno de los dueños de procesos de la empresa • Formato de matriz de riegos. Se realiza la presentación de la matriz de riesgos, estableciendo la información con criticidad alta, media y baja. • Herramienta para medir el estado inicial y final de conocimientos básicos sobre seguridad de la información en la empresa (encuesta). o Se recomienda realizarlo mediante la web, para agilizar el proceso y reducir el costo en tiempo y papelería. o Se decide utilizar la herramienta de Google Drive para la generación web de la encuesta. • Formato utilizado para la presentación de lo política de seguridad de la información. • Los miembros del comité aportan algunas recomendaciones sobre la criticidad de la información y los procedimientos que utilizan para evitar incidentes.	

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

Firmas:

Johana Rodriguez

Laura Triviño (e)

Mauricio Noguera

Diego Nieto

Alexander Ortiz

Guillermo Rodriguez

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Controlado	No		

FORMATO DE ACTAS Y SEGUIMIENTOS

Fecha: Diciembre 26 del 2013	**No. Acta: 07**
Proyecto: Política de seguridad de la información	
Lugar: Instalaciones	
Participantes: Johana Rodriguez Laura Triviño (Encargada) Mauricio Noguera Diego Nieto Alexander Ortiz Guillermo Rodriguez	

Objetivo

Id	Descripción	Res
1	• El oficial de seguridad de la información presentan el primer borrador de la política de seguridad de la información.	

Puntos tratados en la reunión

Id	Descripción	Res
1	• Se envía a la cuenta de correo empresarial el borrador de la primera política de seguridad de la empresa para ser evaluada por los miembros del comité. • Se indica que la metodología para la gestión del riesgo se defina a partir de la criticidad definida en el documento de activos.	

Observaciones

Id	Descripción
	Se solicita una capacitación al personal de la empresa referente a los temas básicos concernientes a la seguridad de la información.

Compromisos

Id	Descripción
	Pendiente definir fecha para la capacitación de seguridad de la información al personal

PROCEDIMIENTOS DEL SISTEMA DE CALIDAD

Documento	GD-FM-NP	Revisión	Mar /2008	Formato de Actas Ingeniería	N/A
Versión	1.0	Confidencialidad	No		

Nombre: Firmas:

Oscar Enrique Carrillo Cante
Sergio Alfonso Rojas
Sandra Patricia Castillo Nordia
Laura Alejandra Trujillo Gómez
Marisol Londoño Galindo
Yohana Herrera R
Jaime F Fonseca
Yuri Alejandra Sosa Rodríguez
Edwar H. Rincon G
Alicia María Londoño Galindo

Anexo 4: Inventario de activos de seguridad de la información de la empresa

DESCRIPCIÓN DEL ACTIVO	TIPO DE ACTIVO	NIVELES DE PROTECCIÓN	RELEVANCIA
Código Fuente (CTLog) Software propio	Software	1	1
Código Fuente (CTMail) Software propio	Software	1	1
Código Fuente (CTMessage) Software propio	Software	1	1
Instaladores	Software	1	1
Código Fuente (CTLog) Software propio	Software	1	1
Código Fuente (CTMail) Software propio	Software	1	1
Código Fuente (Dali) Software propio	Software	1	1
Código Fuente (CTMessage) Software propio	Software	1	1
Código Fuente (IVR) Software propio	Software	1	1
Instaladores y licencias del Software empresarial(Microsoft)	Archivos	2	2
Acta de reuniones	Documentos	3	4

Acta de requerimientos	Documentos	2	3
Scripts SQL	Software	3	3
Instaladores Bases de Datos	Software	1	1
Manuales de productos	Documentos	3	4
Indicadores	Documentos	2	3
Diseños Bases de datos		1	1
Backup Generales (Instaladores de los productos, instaladores bases de datos, codigo fuente, bases de datos de los aplicativos manejados en la empresa, información designada por cada usuario para este fin).	Software	1	1
Cronograma de mantenimiento de los equipos	Documentos	3	4
Hojas de vida de las equipos (Servidores, PCs, portátiles, planta telefónica)	Documentos	3	4
CRM	Software	2	3
Cronograma de soporte para los equipos físicos	Documentos	3	4
Contratos de soporte	Documentos	3	3
Cotizaciones	Documentos	1	1
Actas de entrega	Documentos	3	3
Acuerdos	Documentos	2	3
Lista de Clientes	Documentos	2	3
Lista de precios	Documentos	1	1
Ventas	Documentos	1	3
Órdenes de Compra	Documentos	1	3
Documentación de los proyectos	Documentos	2	3
Facturas	Documentos	1	3
Lista de canales	Documentos	1	3
Convenios con canales y/o clientes	Documentos	1	3
Contratos con clientes	Documentos	1	3
indicadores	Documentos	2	3
Brochures	Documentos	3	3
Datashit	Documentos	3	4
Página Empresarial	Software	2	3
Publicidad	Software	3	4
Redes sociales	Software	3	4
Balances	Documentos	1	1
Certificados	Documentos	2	3
Nomina	Documentos	1	1
Impuestos	Documentos	1	1

Documentos Legales	Documentos	1	1
Reportes ante la Dian	Documentos	1	1
Información DANE	Documentos	1	1
Conciliaciones bancarias	Documentos	1	1
Hojas de vida de los miembros de la organización	Documentos	2	3
Contratos laborales	Documentos	1	3
Formatos ISO	Documentos	2	3
Inventario de activos	Documentos	3	4
Dali	Software	2	3
CTMail	Software	2	3
CTLog	Software	2	3
Antivirus AVG	Software	2	3
Office	Software	2	3
Windows	Software	2	3
Sql Server	Software	2	3
Compras	Documentos	2	3
Visual Studio	Software	2	3
PCs	Hardware	2	3
Portátiles	Hardware	2	3
Servidores	Hardware	1	2
Impresora	Hardware	2	3
Disco Duro USB	Hardware	2	3
Kit Vcam Completo	Hardware	2	3
Celulares	Hardware	2	3
Moden	Hardware	2	3
IMG	Hardware	2	3
Plantas telefónicas	Hardware	1	3
Teléfonos IP	Hardware	2	3
Teléfonos digitales	Hardware	2	3
Hub 24 puertos	Hardware	2	3
UPS	Hardware	2	3
Inventario de PBX Telefónicas	Hardware	2	2
Inventario de Teléfonos IP	Hardware	2	2

Anexo 5. Mapa de riesgos de la empresa

MATRÍZ INVENTARIOS DE ACTIVOS DE LA INFORMACIÓN

PROCESO INGENIERÍA	LÍDER	CARGO	SUBPROCESOS	LÍDER	CARGO	DESCRIPCIÓN DEL ACTIVO	TIPO DE ACTIVO	NIVELES DE PROTECCIÓN	RELEVANCIA
	RICHARD ERAZO PÉREZ	ENGINEERING AND R&D DIRECTOR	INGENIERIA	RICHARD ERAZO PÉREZ	ENGINEERING AND R&D DIRECTOR	Código Fuente (CTLog) Software propio	Software	1	1
						Código Fuente (CTMail) Software propio	Software	1	1
						Código Fuente (CTMessage) Software propio	Software	1	1
			DESARROLLO	ELIER MAURICIO NOGUERA RAMOS	APP DEV MANAGER	Instaladores	Software	1	1
						Código Fuente (CTLog) Software propio	Software	1	1
						Código Fuente (CTMail) Software propio	Software	1	1
						Código Fuente (Dali) Software propio	Software	1	1
						Código Fuente (CTMessage) Software propio	Software	1	1

						Código Fuente (IVR) Software propio	Software	1	1
						Instaladores y licencias del Software empresarial(Microsoft)	Archivos	2	2
			DISEÑO DE APLICACIONES	EDWARD HERNANDO RINCÓN GONZÁLEZ	APPLICATIONS DESIGN MANAGER	Acta de reuniones	Documentos	3	4
						Acta de requerimientos	Documentos	2	3
						Scripts SQL	Software	3	3
						Instaladores Bases de Datos	Software	1	1
						Manuales de productos	Documentos	3	4
						Indicadores	Documentos	2	3
						Diseños Bases de datos		1	1
			SOPORTE	MIGUEL ALEXANDER FUENTES TORRES	TECHNICAL SUPPORT ENGINEER LEADER	Backup Generales (Instaladores de los productos, instaladores bases de datos, código fuente, bases de datos de los aplicativos manejados en la empresa, información designada por cada usuario para este fin).	Software	1	1
						Cronograma de mantenimiento de los equipos	Documentos	3	4

					Hojas de vida de las equipos (Servidores, PCs, portátiles, planta telefónica)	Documentos	3	4
					CRM	Software	2	3
					Cronograma de soporte para los equipos físicos	Documentos	3	4
PROCESO COMERCIAL	DIEGO FERNANDO NIETO	SALES AND MARKETING DIRECTOR	COMERCIAL	NA	NA	Contratos de soporte	Documentos	3	3
						Cotizaciones	Documentos	1	1
						Actas de entrega	Documentos	3	3
						Acuerdos	Documentos	2	3
						Lista de Clientes	Documentos	2	3
						Lista de precios	Documentos	1	1
						Ventas	Documentos	1	3
						Órdenes de Compra	Documentos	1	3
						Documentación de los proyectos	Documentos	2	3
						Facturas	Documentos	1	3
						Lista de canales	Documentos	1	3
						Convenios con canales y/o clientes	Documentos	1	3
						Contratos con clientes	Documentos	1	3

					indicadores	Documentos	2	3
					Brochures	Documentos	3	3
					Datashit	Documentos	3	4
					Pagina Empresarial	Software	2	3
					Publicidad	Software	3	4
					Redes sociales	Software	3	4
PROCESO ADMINISTRATIVO	JOHANNA MARCELA RODRÍGUEZ MUÑOZ	ADMINISTRATIVE AND FINANCIAL DIRECTOR	CONTABILIDAD	NINI JOHANNA		Balances	Documentos	1	1
						Certificados	Documentos	2	3
						Nomina	Documentos	1	1
						Impuestos	Documentos	1	1
						Documentos Legales	Documentos	1	1
						Reportes ante la Dian	Documentos	1	1
						Información DANE	Documentos	1	1
						Conciliaciones bancarias	Documentos	1	1
			RECURSOS HUMANOS	LEIDY JULIETTE ORTÍZ VASQUEZ	ADMINISTRATIVE AND FINANTIAL ASSISTANT	Hojas de vida de los miembros de la organización	Documentos	2	3
						Contratos laborales	Documentos	1	3
						Formatos ISO	Documentos	2	3
						Inventario de activos	Documentos	3	4

			ADMINISTRATRIVO	JOHANNA MARCELA RODRÍGUEZ MUÑOZ	ADMINISTRATIVE AND FINANCIAL DIRECTOR	Dali	Software	2	3
						CTMail	Software	2	3
						CTLog	Software	2	3
						Antivirus AVG	Software	2	3
						Office	Software	2	3
						Windows	Software	2	3
						SQL Server	Software	2	3
						Compras	Documentos	2	3
						Visual Studio	Software	2	3
						PCs	Hardware	2	3
						Portátiles	Hardware	2	3
						Servidores	Hardware	1	2
						Impresora	Hardware	2	3
						Disco Duro USB	Hardware	2	3
						Kit Vcam Completo	Hardware	2	3
						Celulares	Hardware	2	3
						Modem	Hardware	2	3
						IMG	Hardware	2	3
						Plantas telefónicas	Hardware	1	3

						Teléfonos IP	Hardware	2	3
						Teléfonos digitales	Hardware	2	3
						Hub 24 puertos	Hardware	2	3
						UPS	Hardware	2	3
						Inventario de PBX Telefónicas	Hardware	2	2
						Inventario de Teléfonos IP	Hardware	2	2

NIVEL DE PROTECCIÓN	
1	ALTO
2	MEDIO
3	BAJO

RELEVANCIA	
1	CRÍTICA
2	MUY IMPORTANTE
3	IMPORTANTE
4	POCO IMPORTANTE
5	BAJA